KOREAN PATENT ABSTRACT (KR)

PUBLICATION

(51) IPC Code: G06F 17/00
(11) Publication No.: P2002-0003380 (43) Publication Date: 12 January 2002
(21) Application No.: 10-2001-7012831 (22) Application Date: 8 October 2001
(86) International Application No.: PCT/EP2001/00511
(86) International Application Date: 18 January 2001
(87) International Publication No.: WO 2001/59549
(87) International Publication Date: 16 August 2001

(71) Applicant:
KONINKLIJKE PHILIPS ELECTRONICS N.V.

(72) Inventor:
EPSTEIN, Michael, A. et al.

(54) Title of the Invention:

METHODS AND APPARATUS FOR SECURE CONTENT DISTRIBUTION

Abstract:

Methods and apparatus for secure distribution of music and other types of content. The invention allows content to be registered with a centralized trusted registration authority (TRA) in such a way that it can be distributed anonymously, such that the identity of the content provider need not be disclosed until a dispute arises. A first illustrative embodiment of the invention provides unbound rights management, i.e., secure registration of content such that usage rights for the content are not bound to the content itself. In this embodiment, distributed content is not protected by encryption, i.e., confidentiality of content is not provided. However, the content is protected against piracy, due to the fact that the content provider is certified by the TRA, and thus can be traced or otherwise identified in the event that irregularities are detected. Since the usage rights are not bound to the content, the content provider can change the usage rights after the content has been registered with the TRA. Content distribution in second and third illustrative embodiments of the invention provides unbound and bound rights management, respectively, with encryption-based content confidentiality.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
G06F 17/00

(11) 공개번호 특2002-0003380
(43) 공개일자 2002년01월12일

(21) 출원번호 10-2001-7012831
(22) 출원일자 2001년10월08일
번역문 제출일자 2001년10월08일
(86) 국제출원번호 PCT/EP2001/00511
(86) 국제출원출원일자 2001년01월18일
(87) 국제공개번호 WO 2001/59549
(87) 국제공개일자 2001년08월16일

(81) 지정국 국내특허 : 중국, 일본, 대한민국,
EP 유럽특허: 오스트리아, 벨기에, 스위스, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴, 핀랜드, 사이프러스, 터어키,

(30) 우선권주장 09/498,883 2000년02월07일 미국(US)

(71) 출원인 코닌클리케 필립스 일렉트로닉스 엔.브이.
요트.게.아. 롤페즈
네델란드왕국, 아인드호펜, 그로네보드스베그 1

(72) 발명자 엡스타인마이클에이
네델란드왕국,엔엘-5656아아아인드호반,프로프.홀스트란6
로스너마틴
네델란드왕국,엔엘-5656아아아인드호반,프로프.홀스트란6
스타링안토니우스에이.엠.
네델란드왕국,엔엘-5656아아아인드호반,프로프.홀스트란6

(74) 대리인 이병호

심사청구 : 없음

(54) 안전한 콘텐트 분배를 위한 방법 및 장치

요약

본 발명은 음악 및 다른 형식의 콘텐트의 안전한 분배를 위한 방법들 및 장치에 관한 것이다. 본 발명은 콘텐트가 익명으로 분배될 수 있는 방식으로 중앙화된 위탁 등록 기관(TRA)에 등록되는 것을 허용하여, 콘텐트 제공자의 신원은 분쟁일 발생할 때까지 개시될 필요가 없다. 본 발명의 제 1 예시적 실시예는 묶이지 않은 권리들 관리, 즉 콘텐트의 안전한 등록을 제공하여, 콘텐트에 대한 이용 권리들은 콘텐트 자체에 묶이지 않는다. 이 실시예에서, 분배된 콘텐트는 암호

화에 의해 보호되지 않으며, 즉 콘텐트의 비밀성은 제공되지 않는다. 그러나, 콘텐트는, 콘텐트제공자가 TRA에 의해 인증된다는 사실로 인해, 침해에 대해 보호되고, 그래서 불규칙들이 검출되는 경우에 추적되거나 식별될 수 있다. 이용 권리들은 콘텐트에 묶이지 않으므로, 콘텐트 제공자는 콘텐트가 TRA에 등록된 후에 이용 권리들을 변경할 수 있다. 본 발명의 제 2 및 제 3 실시예들에서의 콘텐트 분배는, 암호화에 기초한 콘텐트 비밀성으로, 묶이지 않은 권리들과 묶인 권리들을 각각 제공한다.

대표도
도 1

색인어
위탁 등록 기관, 콘텐트 제공자, 콘텐트 분배

명세서

기술분야

본 발명은, 일반적으로, 안전한 통신(secure communication)의 분야에 관한 것이며, 특히, 네트워크 또는 다른 통신 매체를 통한 음악 및 다른 형식들의 콘텐트(content)의 안전한 전자 분배를 위한 기술들에 관한 것이다.

안전(Security)은 인터넷과 같은 글로벌 통신 네트워트들을 통한 음악 또는 다른 형식들의 콘텐트의 전달에서 점점 중요해진 관심사이다. 특히, 그와같은 네트워크에 기초한 콘텐트 전달 시스템들의 성공적인 수행은 콘텐트 제공자(content provider)들이 적절한 저작권 사용료(copyright royalty)들을 받고, 전달된 콘텐트가 저작권 침해되거나 불법적으로 이용될 수 없다는 것을 보장하는데 대부분 의존하고 있다.

배경기술

음악 콘텐트의 전달에 관하여, 안전한 디지털 음악 주도(Secure Digital Music Initiative) (SDMI)로 알려진 협동적 개발 노력이 선도적 레코딩 산업계와 기술 회사들에 의해 최근에 형성되었다. SDMI의 목표는 디지털 음악 안전을 위한 개방되고 상호운용 가능한(interoperable) 구조의 개발이다. 이것은 양질의 디지털 음악에의 편리한 접근가능성에 대한 소비자 요구에 응답할 것이며, 반면에 또한 콘텐트 개발 및 전달에서의 투자를 보호하도록 저작권 보호를 제공한다. SDMI는 휴대용 음악 장치들에 대한 표준 명세를 이미 만들었으며, SDMI 휴대용 장치 명세(SDMI Portable Device Specification), Part 1, Version 1.0, 1999에 기재되어 있다. SDMI의 장기간의 노력은 모든 형태로의 디지털 음악의 전달을 위한 전체적 구조의 완성을 향해 현재 작용하고 있다.

발명의 상세한 설명

SDMI 및 다른 진행중인 노력들에도 불구하고, 음악 및 다른 콘텐트의 안전한 분배를 위한 현존하는 기술들은 다수의 현저한 결점들이 있다. 예를들어, 많은 그와같은 기술들은 콘텐트 제공자가, 콘텐트 전달시에, 콘텐트 소비자에게 명백히 식별되는 것을 요구하며, 즉 이러한 기술들은 일반적으로 콘텐트 제공자가, 논의(dispute)가 없을 때, 완전히 익명으로 남아있는 것을 허용하지 않는다. 유감스럽게도, 이런 형식의 장치는 어떤 응용들, 특히 개인들이거나 작은 사업체들인 콘텐트 제공자들에 대해서 바람직하지 않거나 비용 효과적이지 않을 수 있다. 다른 예로서, 종래의 기술들은 일반적으로, 그에의해 모든 콘텐트 제공자들이 그들의 작업을 안전하게 등록할 수 있는, 중앙화된 구조를 제공하지 않는다. 그러므로, 콘텐트 제공자들은 이러한 현존하는 기술들하에서 동등하게 취급되지 않으며, 즉, 복잡한 안전 표준들의 수행과 연관된 비용을 낼 수 있는 더 큰 제공자들이 더 작은 제공자들에 대해 유리하다.

상기 내용으로부터 분명한 바와같이, SDMI-추종(compliant) 음악 및 다른 형식들의 내용을 분배하기 위한 개선된 기술들에 대한 수요가 존재한다.

본 발명은 음악 및 다른 형식들의 콘텐트의 안전한 분배를 위한 방법들 및 장치를 제공한다. 본 발명은, 콘텐트가 익명으로 분배될 수 있는 방식으로, 중앙화된 위탁 등록 기관(trusted registration authority)(TRA)에 콘텐트가 등록되는 것을 허용하여, 콘텐트 제공자의 식별은 논의가 발생할 때까지 나타낼 필요가 없다.

본 발명의 제 1 예시적 실시예에서의 콘텐트 분배는, 묶이지 않은(unbound) 권리들 관리, 즉, 콘텐트의 안전한 등록을 제공하는 콘텐트 분배 프로토콜에 따라 수행되어, 콘텐트의 이용 권리들은 콘텐트 자체에 묶이지 않는다. 이 실시예에서, 분배된 콘텐트는 암호화(encryption)에 의해 보호되지 않으며, 즉 콘텐트의 비밀성 (confidentiality)은 제공되지 않는다. 그러나, 콘텐트는, 콘텐트 제공자가 TRA에 의해 인증된다는 사실로 인해, 침해에 대해 보호되며, 그래서 불규칙들이 검출될 때 추적되거나 식별될 수 있다. 이용 권리들이 콘텐트에 묶이지 않으므로, 콘텐트 제공자는 콘텐트가 TRA에 등록된 후에 이용 권리들을 변화시킬 수 있다. 본 발명의 제 2 및 제 3 예시적 실시예들에서의 콘텐트 분배는, 암호화에 기초한 콘텐트 비밀성으로 각각 묶이고 묶이지 않은 권리들 관리를 제공하는 콘텐트 분배 프로토콜들에 따라 수행된다.

유리하게, 본 발명의 콘텐트 분배 방법들 및 장치는 모든 콘텐트 제공자들에 대한 편리하고, 효율적이며, 비용 효과적인 보호를 제공할 수 있다. 본 발명의 이러한 및 다른 특징들과 장점들은 첨부된 도면들과 다음의 상세한 서술로부터 더 분명해질 것이다.

도면의 간단한 설명

도 1은 본 발명에 따른 묶이지 않은 권리들 관리를 지닌 콘텐트 분배 방법을 예시한 도면.

도 2, 도 3, 도 4, 도 5 및, 도 6은 도 1의 콘텐트 분배 방법에서 수행된 처리 동작들을 예시하는 흐름도들.

도 7은 본 발명에 따른 묶이진 않은 권리들과 콘텐트 비밀성을 지닌 콘텐트 분배를 예시한 도면.

도 8, 도 9, 도 10 및, 도 11은 도 7의 콘텐트 분배 방법에서 수행된 처리 동작들을 예시한 흐름도.

도 12는 본 발명에 따른 묶인 권리들 관리 및 콘텐트 비밀성을 지닌 콘텐트 분배 방법을 예시한 도면.

도 13, 도 14, 도 15, 도 16, 도 17 및, 도 18은 도 12의 콘텐트 분배 방법에서 수행된 처리 동작들을 예시한 흐름도들.

실시예

본 발명은 음악 또는 임의의 다른 형식의 콘텐트가 익명으로 분배될 수 있는 방식으로 등록되는 것을 허용한다. 하기에 서술된 콘텐트 분배 방법들은 콘텐트 제공자들이 그 분배전에 위탁 기관에 그 콘텐트를 등록하는 것을 허용하며, 그에 의해 논의가 일어날 때까지 콘텐트 제공자가 나타날 필요없는 방식으로 콘텐트 제공자로부터 콘텐트 소비자에게 콘텐트가 분배되는 것을 허용한다. 유리하게, 본 발명의 콘텐트 분배 방법들은 모든 콘텐트 제공자들을 위한 편리하고, 효율적이며, 비용 효과적인 보호를 제공할 수 있다.

본 발명의 3개의 예시적인 실시예들은 하기에 서술될 것이며, 상술된 기능성 (functionality)을 수행하는 특별한 프로토콜에 각각 대응한다. 프로토콜들은 콘텐트 제공자에게 주어진 제어 및 안전의 레벨에서 변한다. 다음의 서술에서, 동작 E{K}[S]는 키(K)를 이용하여 괄호안의 양(S)의 암호화(encryption)를 표시하고, 동작 D{K}[S]는 키(K)를 이용하여 괄호안의 양(S)의 복호화(decryption)를 표시한다. 하기에 서술될 프로토콜들은 이러한 암호화 및 복호화 동작들을 수행하기 위해 종래의 공용 키 암호 기술(public key cryptography techniques)들을 이용할 수 있다. 일반적으로, 여기에 서술된 예시적인 실시예들에 대해서, 암호화 및 복호화를 위한 비대칭 알고리즘들은 그 첨자열에 " Pub" 또는 " Prv" 를 포함하는 키들을 위해 이용되고, 반면에 대칭 알고리즘들은 하기에 서술될 모든 다른 키들, 예를들어, K_{Cont} 와 $K_{License}$ 를 위해 이용된다. 본 발명에서의 이용에 적합한, 이러한 및 다른 암호화 및 복호화 기술들은 당업자에게 잘 알려져 있으며, 그러므로 여기에서 상세히 서술되지는 않는다.

도 1은 본 발명의 제 1 예시적 실시예에 따라, 묶이지 않은 권리들 관리로 콘텐트를 분배하기 위한 기본적 프로토콜이다. 이 도면은 인증 기관(certificate authority) (CA) (102), 콘텐트 제공자(104), 위탁 등록 기관(106) 및, 콘텐트 소비자 (108)사이의 상호작용들을 도시한다. CA(102), 콘텐트 제공자(104) 및, 콘텐트 소비자 (108)는 또한 본 명세서에서 문자들(X, G 및, C)에 의해 각각 표시된다. 도 1에 예시된 방법은 처리 동작들(110, 120, 130, 140 및, 150)을 포함하고, 이것들은 도 2, 도3, 도 4, 도 5 및, 도 6의 흐름도들에 각각 더 자세히 예시되어 있다.

도 1에서의 처리 동작들은 분배된 콘텐트가 암호화에 의해 보호되지 않는 기본 프로토콜을 수행하며, 즉, 콘텐트의 비밀성은 제공되지 않는다. 그러나, 콘텐트는, 콘텐트 제공자(G)가 TEA(106)에 의해 인증된다는 사실로 인해, 침해에 대해 보호되고, 그래서, 불규칙들이 검출되는 경우에 추적되거나 그렇지않으면 식별될 수 있다. 또한, 본 발명의 실시예에서, 이용 권리들을 콘텐트에 묶이지 않는다. 이것은, 콘텐트가 TRA(106)에 등록된 후에, 콘텐트 제공자(G)가 이용 권리들을 변경하는 것을 허용한다.

도 1의 기본 프로토콜에서, 콘텐트 제공자(104) (G)는 첫째로 CA(102(X)로부터 인증(certificate)을 요청한다. CA(102)는, 도 2에 예시된, 동작(110)에서의 인증을 발생시킨다. 인증 발생 처리는, 예를들어, 설립된 표준에 따라, 종래의 방식으로 실행될 수 있다. 단계(111)에서, CA(102)는, 요청자(requestor) (G)가 그들이 자신이라고 말하는 자인지를 결정한다. 그렇지 않다면, 인증은 발행되지 않는다. 요청자(G)가, 그들이 자신이라고 말하는, 누구인 것으로 결정되면, 단계(112)에서의 CA(102)는 요청자를 위한 공용키 쌍을 발생시키고, 단계(113)에서 요청자(G)에게 개인용키($K_{Prvrequestor}$)를 안전하게 준다. 그다음에, CA(102)는, 단계(114)에 도시된 바와같이, 요청자($I_{requestor}$)의 식별과 인증된 요청자의 공용키($K_{Pubrequestor}$)를 묶고, 도 1에 도시된 바와같이 요청자(G)에 인증($Cert_X(I_G, K_{PubG})$)을 발생한다. 인증들을 위한 요청들이 각각의 거래(transaction)에 대해서 강제적이지 않으며, 즉, 한번 어떤사람이 인증을 얻으면 만료될 때까지 재사용될 수 있다는 것이 유의되어야 한다.

도 1의 동작(120)은 도 3에 예시되어 있다. 단계(121)에서 콘텐트 제공자(G)는 특정 콘텐트(M)에 대한 해시(hash) 값을 발생시킨다.

$H = hash(M)$

그다음에, 단계(122)에서 콘텐트 제공자(G)는 그 개인용키(K_{PrvG})를 이용하여 H를 암호화하고,

$H' = E\{K_{PrvG}\}[H]$

단계(123)에서 Q를 다음과 같이 발생시킨다.

$Q = (H', Cert_X(I_G, K_{PubG}))$

그다음에, 콘텐트 제공자(G)는, 도 1에 도시된 바와같이, Q를 등록하도록 TRA(106)에 요청을 보낸다.

도 4는 TRA(106)에 의해 수행된 동작(103)을 도시한다. 단계(131)에서, TRA는 콘텐트 제공자(G)에 대한 인증 C ert$_X$(I_G, K_{PubG})이 유효한지를 결정한다. 그렇지 않다면, 동작은 종료하고, Q의 등록에 대한 요청은 거부된다. 단계(131)에서 인증이 유효한것으로 결정된다면, 단계(132)에서 TRA는 수신(receipt)의 날짜 및 시간뿐 아니라 H' 및 I_G 쌍도 저장한다. 단계(133)에서, TRA는 다음과 같이 Q로부터 해시 값 H를 추출한다.

$H = D\{K_{PubG}\}[H']$

그다음에, 단계(134)에서 TRA는 다음과 같이 등록 스터브(stub)(Q')를 발생시킨다.

$Q' = E\{K_{PrvTRA}\}[H]$

그래서, TRA는 콘텐트 제공자(G)에 의해 전송된 해시 값(H)을 복호화하고, 그것을 개인용 키 K_{PrvTRA} 로 재-암호화한다. 결과적인 등록 스터브(Q')는, 도 1에 도시된 바와같이, 콘텐트 발신자(originator)(G)로 발행된다.

그다음에, 도 1의 동작이 콘텐트 제공자(G)에 의해 수행된다. 도 5는 이 동작을 더 자세히 도시한다. 콘텐트 제공자(G)는, 임의의 종래 방식으로, TRA에 대한 인증을 얻는 것으로 가정된다. 단계(141)에서, 콘텐트 제공자(G)는 TRA에 대한 인증이 유효한지를 결정한다. 그렇지 않다면, 동작은 종료한다. TRA에 대한 인증이 유효하다면, 콘텐트 제공자는 단계(142)에서,

$D\{K_{PubTRA}\}[Q'] = hash(M)$ 인지를 결정한다.

상기 식이 성립한다면, Q'과 M은 후속 분배를 위해 단계(143)에 저장된다. 성립하지 않으면, 동작은 Q'과 M을 저장하지 않고 종료한다. Q'과 M이 저장된다면, 콘텐트 제공자는 콘텐트(M)에 대한 등록 처리가 성공적으로 완료되었다는 것을 알게되고, 그러므로 콘텐트 제공자는 콘텐트를 하나이상의 소비자들에게 분배하는데 있어 자유롭다.

도 1을 다시 언급하면, 동작(140)의 성공적인 완료 이후에, 콘텐트 제공자는 등록 스터브 (Q')와 콘텐트(M)를 콘텐트 소비자(108)(C)에게 분배한다. 도 6은 콘텐트 소비자(C)에 의해 수행된 바와같은 동작(150)을 도시한다. 콘텐트 소비자는 단계 (151)에서 TRA에 대한 인증이 유효한지를 결정한다. 유효하지 않다면, 동작은 종료한다. 유효하다면, 콘텐트 제공자는 단계(152)에서,

$D\{K_{PubTRA}\}[Q'] = hash(M)$ 인지를 결정한다.

상기 식이 성립하지 않는다면, 동작은 종료한다. 성립한다면, 콘텐트 소비자(C)는 단계(153)에서 콘텐트(M)를 재생 및/또는 저장한다. 그래서, 콘텐트 소비자(C)는 콘텐트 제공자(G)가 " 진실(bona fide)" 로서 유효하게 된 경우에만 콘텐트를 수신한다.

콘텐트 소비자에 의해 수행된 바와같은, 동작(150)과 본 명세서에 서술된 다른 동작들은 부정조작이 불가능하거나(tamper-proof) 부정조작되기 어려운(tamper-resistant) 장치에서 수행될 수 있으며, 예를들어 콘텐트가 콘텐트 소비자에 의해 복호화될 때, 복호화된 콘텐트는 승인되지 않은 이용자들 및 장치들에 접근가능하지 않아야 한다는 것을 유의해야 한다.

이전에 언급된 바와같이, 콘텐트(M)는 음악 또는 다른 형식의 콘텐트일 수 있다. 그것은, 임의의 적당한 코딩 장치를 이용하여 발생된, 압축된 포맷 또는 압축되지 않은 포맷에 있을 수 있다. 단일 콘텐트 소비자로의 보증된 분배가, 당업자에게 분명한 바와같이, 종래의 안전 링크 프로토콜을 이용하여 수행될 수 있다.

잠재적인 보호 문제는, 콘텐트 소비자가 등록 스터브(Q')를 동반한 콘텐트뿐 아니라 레거시(legacy) 콘텐트를 재생할 수 있다면, 상술한 기본 프로토콜에서 발생할 수 있다. 즉, Q'이 분실되거나 존재하지 않는다면, 기본 프로토콜에서 등록된 콘텐트와 레거시 콘텐트를 구분할 방법이 없게 된다.

이하에 서술될 프로토콜의 향상된 버젼들에서, 암호화된 포맷은 구별 (distiction)을 제공하며, 그래서 보호 문제는 일반적으로 이슈가 아니다. 그러나, 보호 문제는 콘텐트(M)에서 삽입된 워터마크(enbedded watermark)를 제공하여 기본 프로토콜에서 해결될 수 있다. 이러한 삽입된 워터마크는, 콘텐트가 재생될 수 있기 전에 유효 등록 스터브(Q')가 존재해야 한다는 것을 콘텐트 소비자에세 표시한다. 그와같은 실시예에서, 도 6에 예시된 동작(150)은, Q'이 존재해야 한다는 것을 표시하는 워터마크를 M이 포함하는지를 결정하는 부가적 처리 단계를 단계(151)전에 포함하도록 수정된다. 그렇다면, 동작은 단계(151)에서 계속된다. 그러한 워터마크가 없다면, 동작은 단계들(151과 152)을 건너뛰어, 단계(153)로 진행한다. 다른 구성들도 가능한데, 예를들어, 삽입된 워터마크를 위한 상술된 부가적 처리 단계는 도 6의 처리 단계들(151과 152)사이에서 수행될 수 있다.

삽입된 워터마크는 유효 등록 스터브, 및 가능하게는 스터브의 종류, 예를들면, hash(M) 등이 존재해야 한다는 것을 표시할 필요만 있다는 것을 유의해야 한다. 그러므로, 삽입된 워터마크는 등록 스터브 자체를 포함할 필요는 없다. 부가하면, 그와같은 워터마크는, 기본 프로토콜만을 지원하는 장치들로의 콘텐트의 기록 및 분배를 방지하도록, 하기에 서술된 바와같은 프로토콜의 향상된 버젼을 이용하여 분배된 콘텐트에서 이용될 수도 있다는 것을 유의해야 한다.

도 7은 본 발명의 제 2 예시적 실시예에 따른 콘텐트 비밀성과 묶이지 않은 권리들 관리를 지닌 콘텐트 분배 방법을 예시한다. 이 도면은, CA(Y)로 또한 언급되는, 부가적 인증 기관(CA)(200), 실체들(CA)(X)(102), 콘텐트 제공자(104), TRA(106) 및 콘텐트 소비자(108)사이의 상호작용들을 도시한다. 도 8, 도 9, 도 10 및 도 11은 도 7의 콘텐트 분배 방법에서 수행된 처리 동작들을 예시하는 흐름도들이다. 도 7에 예시된 방법은 처리 동작들(210, 220, 250, 260 및 270)을 포함한다. 처리 동작(210)은 일반적으로 도 2의 동작(110)에 대응하지만, CA(Y)(200)에 의해 수행된다. 처리 동작들(220, 250, 260 및, 270)은 도 8, 도 9, 도 10 및 도 11의 흐름도들에 각각 더 자세히 예시되어 있다.

도 7에서의 처리 동작들은 도 1의 기본 프로토콜의 향상된 버젼을 수행한다. 이러한 향상된 프로토콜에서, 콘텐트는 암호화에 의해 보호되며, 즉, 콘텐트 비밀성이 제공된다. 부가하면, 이미 서술된 기본 프로토콜에서와 같이, 향상된 프로토콜에서의 콘텐트는 또한 침해로부터 보호되고, 이용 권리들은 콘텐트에 묶이지 않으며, 콘텐트가 등록된 후에 발행자(publisher)가 이용 권리들을 변화시키는 것을 허용한다.

도 7의 향상된 프로토콜에서, 콘텐트 제공자(G)(104)는 CA(X)(102)로부터 인증을 요청하고, 콘텐트 소비자(C)(108)는 CA(Y)(200)로부터 인증을 요청한다. CA(102, 200)들은, 동작들(110과 210) 각각에서, 인증들 $Cert_X(I_G, K_{PubG})$, $Cert_Y(I_C, K_{PubC})$를 각각, 도 2와 연결하여 이미 서술된 방식으로 발생시킨다. 인증 $Cert_X(I_G, K_{PubG})$는 CA(102)에 의해 콘텐트 제공자(G)로 발행되고, 인증 $Cert_Y(I_C, K_{PubC})$는 CA(200)에 의해 콘텐트 제공자(C)로 발행된다. CA(102)와 CA(200)는 동일한 CA일 수 있다는 것을 유의해야 한다. 이러한 예에서, 이것들은 인증들이 동일한 CA로부터 올 필요는 없다는 것을 예시하도록 별개의 실체들로서 도시된다.

도 7의 동작(220)은 도 8에 예시되어 있다. 단계(221)에서, 콘텐트 제공자(G)는 암호화된 콘텐트(M')를 발생시키도록 콘텐트(M)를 암호화한다.

$$M' = E\{K_{Cont}\}[M]$$

K_{Cont} 는 단일 키일 필요는 없다는 것을 유의해야 한다. 예를들어, 그것은 키들이 순차일 수 있으며, 여기서 각각의 키들은 콘텐트의 서로다른 부분들을 암호화하도록 이용된 순차로 되어 있다. 콘텐트 제공자(G)(222)는 단계(222)에서 특정 콘텐트(M')에 대한 해시 값을 발생시킨다.

$$H = hash(M')$$

그다음에, 콘텐트 제공자(G)는 단계(223)에서 개인용 키(K_{PrvG})를 이용하여 H를 암호화하고,

$$H' = E\{K_{PrvG}\}[H]$$

단계(224)에서 다음과 같이 Q를 발생시킨다.

$Q = (H', Cert_X(I_G, K_{PubG}))$

그다음에, 콘텐트 제공자(G)는, 도 7에 도시된 바와같이, Q를 등록하도록 TRA(106)에 요청을 전송한다. 요청이 도 4에 예시된 바와같이, 동작(130)에서 TRA(106)에 의해 처리되고, 등록 스터브(Q')가 TRA(106)에 의해 콘텐트 제공자(G)로 발행된다.

그다음에, 콘텐트 제공자(G)는, M이 단계들(142와 143)에서 M'에 의해 대체된다는 것을 제외하면, 도 5의 동작(140)과 동일한, 동작(140')을 수행한다. 저장된 Q'과 M'은 조건 체크(142)의 결과이다. (142)가 참이면 Q'과 M'이 저장되고 콘텐트 제공자(G)는 암호화된 콘텐트(M')에 대한 등록 처리가 성공적으로 완료되었다는 것을 알게된다. 그러므로, 콘텐트 제공자는 암호화된 콘텐트를 하나이상의 소비자들에게 분배하는데 있어 자유롭다.

도 7을 언급하면, 동작(140')의 성공적인 완료 이후에, 콘텐트 제공자(G)는 등록 스터브(Q')와 암호화된 콘텐트(M')를 콘텐트 소비자(108)(C)에게 분배한다.

도 9는 콘텐트 소비자(C)에 의해 수행된 바와같은 동작(250)을 도시한다. 콘텐트 소비자(C)는 단계(251)에서 TRA에 대한 인증이 유효한지를 결정한다. 유효하지 않다면, 동작은 종료한다. 유효하다면, 콘텐트 소비자는 단계(252)에서, 하기 수식이 성립하는지를 결정한다.

$D\{K_{PubTRA}\}[Q'] = hash(M')$

상기 식이 성립하지 않는다면, 동작은 종료한다. 성립한다면, 콘텐트 소비자(C)는 암호화된 콘텐트(M')를 단계(253)에서 저장한다. 그래서, 콘텐트 소비자(C)는, 콘텐트 제공자(G)가 " 진실 (bona fide)" 로서 유효하게 된 경우에만, 암호화된 콘텐트를 저장한다.

콘텐트를 액세스하기 위해, 콘텐트 제공자(C)는 발신자(originator)에 의해 정의된 이용 규칙들뿐아니라 콘텐트 복호화 키(K_{Cont})도 또한 수신해야 한다. 이 정보는 콘텐트 제공자(G)에 의한 소비자 식별의 성공적인 입증후에만 콘텐트 소비자(C)에게 전송된다. 이 목적을 위해, 콘텐트 소비자(C)는 동작(250)의 단계(254)에서 암호화된 콘텐트(M')에 대한 해시 값을 발생시킨다.

$H = hash(M')$

그다음에, 콘텐트 소비자는 단계(255)에서 개인용 키(K_{PrvC})를 이용하여 H를 암호화하고,

$H'' = E\{K_{PrvC}\}[H]$

단계(256)에서 암호화된 해시값과 상기 언급된 인증 $Cert_Y(I_C, K_{PubC})$를 포함하는 한 쌍인 Q" 을 발생시킨다.

$Q'' = (H'', Cert_Y(I_C, K_{PubC}))$.

그다음에, 한 쌍인 Q" 은 콘텐트 소비자(C)로부터 콘텐트 제공자(G)로 전송된다.

도 10은 콘텐트 제공자(G)에 의해 수행된 동작(260)을 도시한다. 단계(261)에서, 콘텐트 제공자(G)는 콘텐트 소비자(C)의 인증 $Cert_Y(I_C, K_{PubC})$이 유효한지를 결정한다. 유효하지 않다면, 동작은 종료한다. 유효하다면, 콘텐트 제공자(G)는 단계(262)에서, 하기 수식이 성립하는지를 결정한다.

$D\{K_{PubC}\}[H''] = hash(M')$

상기 식이 성립하지 않는다면, 동작은 종료한다. 성립한다면, 콘텐트 제공자(G)는 단계(263)에서 콘텐트 키(K_{Cont})와 이용 규칙들을 암호화하도록 라이센스 키($K_{license}$)를 이용하고,

$A = E\{K_{license}\}[usage\_rules \mid K_{Cont}]$

단계(264)에서 라이센스 키를 암호화한다.

$B = E\{K_{PubC}\}[K_{license}]$

그다음에, 라이센스 스터브(L)는 단계(265)에서 상기 쌍(A, B)으로서 발생된다. 그다음에, 도 7에 도시된 바와같이, 콘텐트 제공자(G)는 라이센스 스터브(L)를 콘텐트 소비자(C)에게 전송한다.

도 11은 라인센스 스터브(L)의 수신시에 콘텐트 소비자(C)에 의해 수행된 동작(270)을 도시한다. 단계(271)에서, 콘텐트 소비자(C)는 라이센스 키를 복호화하고,

$K_{license} = D\{K_{PrvC}\}[B]$

그다음에, 단계(272)에서 규칙들과 콘텐트 키를 복호화한다.

$usage\_rules \mid K_{Cont} = D\{K_{license}\}[A]$

그다음에, 콘텐트 소비자(C)는 암호화된 콘텐트(M')를 단계(273)에서 복호화한다.

$M = D\{K_{Cont}\}[M']$

그다음에, 콘텐트 소비자는 단계(274)에서 이용 규칙들을 콘텐트(M)에 적용하고, 단계(275)에서 콘텐트(M)를 재생 및/또는 저장한다.

도 12는 본 발명의 제 3 의 예시적인 실시예에 따른 콘텐트 비밀성 및 묶인 권리들 관리를 지닌 콘텐트 분배 방법을 예시한다. 이 도면은 실체들 CA(Y) (200), CA(X) (102), 콘텐트 제공자(G) (104), TRA(106) 및, 콘텐트 소비자(C) (108)사이의 상호작용들을 도시한다. 도 13, 도 14, 도 15, 도 16, 도 17 및 도 18은, 도 12의 콘텐트 분배 방법에서 수행된, 처리 동작들(320, 330, 340, 350, 360 및, 370)을 각각 예시하는 흐름도들이다. 처리 동작들(110과 210)은 도 7의 실시예와 연결되어 이전에 서술된 방식으로 수행된다.

도 12에서의 처리 동작들은 도 1의 기본 프로토콜의 대안의 향상된 버전을 수행한다. 이 대안의 향상된 프로토콜에서, 도 7의 향상된 프로토콜에서와 같이, 콘텐트는 암호화에 의해 보호되며, 즉 콘텐트 비밀성이 제공된다. 부가하면, 이전에 서술된 기본적이고 향상된 프로토콜들에서와 같이, 대안의 향상된 프로토콜에서의 콘텐트는 침해로부터 보호된다. 그러나, 이전에 서술된 프로토콜들과 달리, 이러한 대안의 향상된 프로토콜은 또한 라이센스가 확실하다는 것을 보증하는데, 콘텐트와 함께 묶여 있고 TRA(106)로 등록되었기 때문이다.

이러한 접근은 콘텐트 제공자(G)가, 콘텐트가 TRA(106)로 등록된 후에, 콘텐트 이용 규칙들을 변경할 수 없다는 점에서 콘텐트 제공자(G)를 제한한다는 것이 유의되어야 한다. 결과적으로, 콘텐트 제공자(G)가 등록후에 이용 규칙들을 변경하기를 원한다면, 새로운 등록이 필요할 것이다.

도 12의 향상된 프로토콜에서, 콘텐트 제공자(G) (104)는 CA(X) (102)로부터 인증을 요청하고, 콘텐트 소비자(C) (108)는 CA(Y) (200)로부터 인증을 요청한다. CA들 (102, 200)은 동작들(110과 210) 각각에서, 인증들 $Cert_X(I_G, K_{PubG})$, $Cert_Y(I_C, K_{PubC})$을 각각, 도 2와 연결되어 이전에 서술된 방식으로, 발생시킨다. 인증 $Cert_X(I_G, K_{PubG})$은 CA(102)에 의해 콘텐트 제공자(G)로 발행되고, 인증 $Cert_Y(I_{C,PubG})$은 CA (200)에 의해 콘텐트 소비자(C)로 발행된다. 이전에 언급된 바와같이, CA(102)와 CA(200)는 동일한 CA일 수 있다.

도 12의 동작(320)은 도 13에 예시된다. 콘텐트 제공자(G)는 암호화된 콘텐트 (M')를 발생시키도록 단계(321)에서 콘텐트(M)를 암호화한다.

$M' = E\{K_{Cont}\}[M]$

이전에 언급된 바와같이, K_{Cont} 는 단일 키일 필요는 없으며, 예를들어, 키들의 순차일 수 있고, 순차에서의 각각의 키들은 콘텐트의 서로다른 부분들을 암호화하도록 이용된다.

콘텐트 제공자(G)는 단계(322)에서 특정 콘텐트(M')에 대한 해시 값을 발생시킨다.

$H1 = hash(M')$

단계(323)에서, 콘텐트 제공자(G)는 다음과 같이 라이센스 등록 스터브(A)를 발생시켜서 콘텐트 키에 한 세트의 규칙들을 묶는다.

$A = E\{K_{license}\}[usage\_rules \mid K_{Cont}]$

특정 콘텐트 키에 규칙들을 묶는 것은, 상기에 도시된 바와같이 암호화를 통해서, 또는 대안으로 임의의 다른 암호법의 묶는(binding) 메커니즘을 통해서 행해질 수 있다는 것을 유의해야 한다. 암호화를 통해서 행해질 때, 암호화는, 묶임(binding)을 파괴시킬 수 있는 블록 재생 공격(block replay attack)을 방지하도록 연쇄(chaining) 모드를 이용해야 한다.

단계(323)에서의 규칙들의 묶임후에, A의 해시 값이 단계(324)에서 발생된다.

$H2 = hash(A)$

그다음에, 콘텐트 제공자(G)는 단계(325)에서 개인용 키(K_{PrvG})를 이용하여 H1과 H2를 암호화하고,

$H' = E\{K_{PrvG}\}[H1 \mid H2]$

단계(326)에서 다음과 같이 Q를 발생시킨다.

$Q = (H', Cert_X(I_G, K_{PubG}))$

그다음에, 콘텐트 제공자(G)는, 도 12에 도시된 바와같이, Q를 등록하기 위해 TRA(106)에 요청을 전송한다. 요청은, 도 14에 예시된 바와같이, 동작(330)에서 TRA(106)에 의해 처리된다. 단계(331)에서, TRA는 콘텐트 제공자(G)에 대한 인증 $Cert_X(I_G, K_{PubG})$이 유효한지를 결정한다. 유효하지 않다면, 동작은 종료하고, Q의 등록에 대한 요청이 거부된다. 인증이 유효한것으로 단계(331)에서 결정된다면, TRA는 단계(332)에서 수신의 시간 및 날짜 뿐아니라 H'과 I_G 쌍도 저장한다. 단계(333)에서, TRA는 Q로부터 해시 값들(H1과 H2)을 추출한다. 그다음에, TRA는 단계(334)에서 다음과 같이 콘텐트 등록 스터브(Q1')을 발생시키고,

$Q1' = E\{K_{PrvTRA}\}[H1]$

단계(334)에서 다음과 같이 이용 규칙들 등록 스터브(Q2')을 발생시킨다.

$Q2' = E\{K_{PrvTRA}\}[H2]$

그래서, TRA는 콘텐트 제공자(G)에 의해 전송된 해시 값들(H1과 H2)을 복호화하고, 개인용 키(K_{PrvTRA})를 이용하여 그것들을 재-암호화한다. 결과적인 등록 스터브들(Q1'과 Q2')은, 도 12에 도시된 바와같이, 콘텐트 발신자(G)로 발행된다.

그다음에, 도 12의 동작(340)은 콘텐트 제공자(G)에 의해 수행된다. 도 15는 이 동작을 더 자세히 도시한다. 단계(341)에서, 콘텐트 제공자(G)는 TRA에 대한 인증이 유효한지를 결정한다. 유효하지 않다면, 동작은 종료한다. TRA에 대한 인증이 유효하면, 콘텐트 제공자(G)는 단계(142)에서 다음식이 성립하는지를 결정한다.

$D\{K_{PubTRA}\}[Q1'] = hash(M')$

상기 식이 성립한다면, Q1', Q2' 및 M'은 후속 분배를 위해서 단계(343)에서 저장된다. 성립하지 않는다면, 동작은 Q1', Q2' 및, M'을 저장하지 않고서 종료한다. Q1', Q2' 및, M'이 저장되면, 콘텐트 제공자는 암호화된 콘텐트(M')에 대한 등록 프로세스가 성공적으로 완료되었는지를 알게되고, 그러므로 콘텐트 제공자는 하나이상의 소비자들에 콘텐트를 분배하는데 있어 자유롭다.

도 12를 언급하면, 동작(340)의 성공적인 종료후에, 콘텐트 제공자(G)는 등록된 콘텐트 스터브(Q1')와 암호화된 콘텐트(M')를 콘텐트 소비자(108)(C)에게 분배한다.

도 16은 콘텐트 소비자(C)에 의해 수행된 바와같이 동작(350)을 도시한다. 콘텐트 소비자(C)는, 단계(351)에서, TRA에 대한 인증이 유효한지를 결정한다. 유효하지 않다면, 동작은 종료한다. 유효하다면, 콘텐트 소비자(C)는 단계(352)에서 다음식이 성립하는지를 결정한다.

$D\{K_{PubTRA}\}[Q1'] = hash(M')$

상기 식이 성립하지 않는다면 동작은 종료한다. 성립한다면, 콘텐트 소비자(C)는 암호화된 콘텐트(M')를 단계(353)에서 저장한다. 그래서, 콘텐트 소비자(C)는 콘텐트 제공자(G)가 " 진실(bona fide)" 로서 유효한 경우에만 암호화된 콘텐트를 저장한다.

콘텐트를 액세스하기 위해, 콘텐트 소비자(C)는 발신자에 의해 정의된 임의의 이용 규칙들 뿐아니라 콘텐트 암호화 키(K_{Cont})도 수신해야 한다. 이 정보는 콘텐트 제공자 (G)에 의한 소비자 식별의 성공적인 입증후에만 콘텐트 소비자(C)로 전송된다. 이 목적을 위해, 콘텐트 소비자(C)는 동작(350)의 단계(354)에서 암호화된 콘텐트(M')에 대한 해시값을 발생시킨다.

$H = hash(M')$

그다음에, 콘텐트 소비자는 단계(355)에서 개인용 키(K_{PrvC})를 이용하여 H를 암호화하고,

$H'' = E\{K_{PrvC}\}[H]$

단계(356)에서, 암호화된 해시값과 상기 언급된 인증 $Cert_Y(I_C, K_{PubC})$을 포함하는 쌍 Q" 을 발생시킨다.

$Q'' = (H'', Cert_Y(I_C, K_{PubC}))$

그다음에, 쌍 Q" 은 콘텐트 소비자(C)로부터 콘텐트 제공자(G)로 전송된다.

도 17은 콘텐트 제공자(G)에 의해 수행된 동작(360)을 도시한다. 단계(361)에서, 콘텐트 제공자(G)는 콘텐트 소비자(C)의 인증 $Cert_Y(I_C, K_{PubC})$이 유효한지를 결정한다. 유효하지 않다면, 동작은 종료한다. 유효하다면, 콘텐트 제공자(G)는 단계(362)에서 다음식이 성립하는지를 결정한다.

$D\{K_{PubC}\}[H''] = hash(M')$

상기 식이 성립하지 않는다면, 동작은 종료한다. 상기 식이 성립한다면, 콘텐트 제공자(G)는 단계(363)에서 콘텐트 소비자(C)의 공용 키(K_{PubC})를 이용하여 라이센스 키 ($K_{license}$)를 암호화한다.

$B = E\{K_{PubC}\}\{K_{license}\}$

그다음에, 라이센스 스터브(L)는 단계(364)에서 삼중(triple)(A, B, Q2')으로서 발생된다. 그다음에, 도 12에 도시된 바와같이, 콘텐트 제공자(G)는 라이센스 스터브(L)를 콘텐트 소비자(C)에게 전송한다.

도 18은 라이센스 스터브(L)의 수신시에 콘텐트 소비자(C)에 의해 수행된 동작(370)을 도시한다. 단계(371)에서, 콘텐트 소비자(C)는 다음식이 성립하는지를 결정한다.

$D\{K_{PubTRA}\}[Q2'] = hash(A)$

상기 식이 성립하지 않는다면, 처리는 종료한다. 성립한다면, 콘텐트 소비자(C)는 단계(372)에서 라이센스 키를 복호화하고,

$K_{license} = D\{K_{PrvC}\}[B]$

그다음에, 단계(373)에서 규칙들과 콘텐트 키를 복호화한다.

$usage\_rules \mid K_{Cont} = D\{K_{license}\}[A]$

그다음에, 콘텐트 소비자(C)는 단계(374)에서 암호화된 콘텐트(M')를 복호화한다.

$M = D\{K_{Cont}\}[M']$

그다음에, 콘텐트 소비자는 단계(375)에서 이용 규칙들을 콘텐트(M)에 적용하고, 단계(376)에서 콘텐트(M)를 재생 및/또는 저장한다.

상기에 상술된 프로토콜들에서, 콘텐트의 특별한 부분의 불법적 복사, 예를들어, 표절된 음악 선택이 불법적 복사가 SDMI에 추종하도록 하려는 시도로 등록된다면, TRA(106)는 어떤 문제들도 없이 등록을 수행할 것이다. 그러나, 그와 같은 등록은 콘텐트 제공자(G)가 인증을 TRA(106)에 제시하여 그자신을 정확하게 식별하는 것을 요구한다. 그래서, 비록 불법적 복사가 등록되었다 하더라도, 등록을 한 콘텐트 제공자는 즉시 식별되고 수행될 수 있다. 이런 방식으로, 위반자들은 콘텐트가 콘텐트 소비자에 배포된 후와 분쟁이 발생한 경우에만 추적된다. 등록된 콘텐트 제공자의 식별을 위한 근거들은, 동일한 또는 충분히 유사한 콘텐트에 대한 유효하고 앞선 (prior) 등록을 고소인이 제시하는 것을 요구하도록, 합법적으로 정의되어야 한다.

하나 이상의 CA들(102와 200), 콘텐트 제공자(104), TRA(106) 및, 콘텐트 소비자 (108)는 각각, 상술된 프로토콜들과 연관된 처리 동작들을 수행하기 위한, 하나 이상의 개인용 컴퓨터들, 워크스테이션들, 메인프레임 컴퓨터들, 또는 다른 프로세서 에 기초한 장치들을 나타낼 수 있다. 그와같은 프로세서 장치들은 일반적으로 상술된 처리 기능들과 연관된 적당한 소프트웨어 프로그램 지시들을 저장하기 위한 하나이상의 메모리 장치들과, 소프트웨어 프로그램 지시들을 수행하기 위한 적어도 하나의 프로세서를 포함할 것이다. 도 1, 도 7 및, 도 12에 도시된 바와같이, 이러한 실체들사이의 통신들은 인터넷, 넓은 지역 네트워크, 국지적 지역 네트워크, 인트라넷(intranet), 엑스트라넷(extranet) 뿐아니라 이러한 및 다른 네트워크들의 결합과 같은 글로벌 통신을 통해 수행된 네트워크 접속들일 수 있다. 그래서, 도 1, 도 7 및, 도 12는 또한 대응하는 프로토콜들을 수행하기 위한 시스템 처리 소자들사이의 상호접속을 예시하는 시스템 다이어그램들로서 보여질 수 있다.

본 발명의 상술된 실시예들은 예시적인것으로만 의도된다. 예를들어, 본 발명은, 임의의 바람직한 형식의 프로세서에

기초한 장치를 위해서 및, 본 명세서에 서술된 것과 다른 많은 응용들에서, 임의의 바람직한 형식의 소프트웨어 또는 하드웨어 구성요소의 업그레이드 또는 다른 재구성뿐 아니라 이러한 및 다른 구성요소들의 결합을 수행하는데 이용될 수 있다. 본 발명은 또한, 다른 종래의 전자, 자기 또는 광학 저장 매체상에 저장되고, 처리장치에 의해, 예를들어 시스템(200)의 처리기들 (220과 230)에 의해 수행된 하나이상의 소프트웨어 프로그램들의 형태로 적어도 부분적으로 수행될 수 있다. 다음의 청구항들의 범위내에서 이러한 및 다수의 다른 실시예들은 당업자에게 분명할 것이다.

(57) 청구의 범위

청구항 1.

콘텐트 제공자(104)로부터 콘텐트 소비자(108)로의 콘텐트의 분배를 위한 방법에 있어서,

위탁 등록 기관(106)으로의 상기 콘텐트의 등록을 요청하는 단계,

상기 위탁 등록 기관으로부터 등록 정보를 수신하는 단계, 및

상기 콘텐트와 연결하여 상기 콘텐트 소비자에게 상기 등록 정보의 적어도 일부분을 분배하는 단계를 포함하는, 콘텐트 분배 방법.

청구항 2.

제 1 항에 있어서,

상기 위탁 등록 기관으로의 상기 콘텐트의 등록은, 인증 기관(102)으로부터 상기 콘텐트 제공자에 의해 얻어진 인증에 적어도 부분적으로 기초하는, 콘텐트 분배 방법.

청구항 3.

제 1 항에 있어서,

상기 등록 정보는 상기 콘텐트와 연결되어 상기 콘텐트 소비자에게 분배되어, 상기 콘텐트 제공자는, 상기 콘텐트 소비자에게 분배된 상기 등록 정보로부터, 상기 위탁 등록 기관에 의해 후속하여 식별될 수 있는, 콘텐트 분배 방법.

청구항 4.

제 1 항에 있어서,

상기 콘텐트 제공자는 상기 위탁 등록 기관으로부터 상기 등록 정보를 수신하고, 상기 등록 기관의 유효를 결정하고, 상기 등록 기관이 유효하다면, 상기 콘텐트 소비자로의 후속 분배를 위해 상기 콘텐트와 상기 등록 정보를 저장하는, 콘텐트 분배 방법.

청구항 5.

제 2 항에 있어서,

상기 콘텐트 제공자는 특정 콘텐트 M에 대한 해시 값 H를 발생시키고, 암호화된 해시 값 H'을 발생시키도록 그의 개인용 키 K_{PrvG} 를 이용하여 H를 암호화하고, 그다음에 다음식,

$Q = (H', Cert_X(I_G, K_{PubG}))$, (여기서, $Cert_X(I_G, K_{PubG})$는 상기 인증 기관으로부터 얻어진 인증)

와 같이 한 쌍인 Q를 발생시키고, 등록을 위해 상기 위탁 등록 기관에 Q를 전송하는, 콘텐트 분배 방법.

청구항 6.

제 5 항에 있어서,

상기 위탁 등록 기관은 상기 콘텐트 제공자에 대한 인증 $Cert_Y(I_G, K_{PubG})$이 유효한지를 결정하고, 유효하지 않다면 등록을 거부하고, 유효하다면 I_G와 수신의 시간 및 날짜와 함께 상기 암호화된 해시 값 H'을 저장하고, 다음식,

$H = D\{K_{PubG}\}[H']$

과 같이 Q로부터 상기 해시값 H를 추출하고, 그다음에 다음식,

$Q' = E\{K_{PrvTRA}\}[H]$

과 같이 등록 스터브 Q'의 형식으로 상기 등록 정보를 발생시키는, 콘텐트 분배 방법.

청구항 7.

제 6 항에 있어서,

상기 콘텐트 제공자는 상기 위탁 등록 기관으로부터 Q'을 수신하고, 다음식,

$D\{K_{PubTRA}\}[Q'] = hash(M)$

이 성립하는지를 결정하고, 성립한다면 상기 콘텐트 소비자로의 후속 분배를 위해 Q'과 M을 저장하는, 콘텐트 분배 방법.

청구항 8.

제 7 항에 있어서,

상기 콘텐트 소비자는, 상기 콘텐트 제공자로부터의 Q'과 M의 수신시에, 다음식,

$D\{K_{PubTRA}\}[Q'] = hash(M)$

이 성립하는지를 결정하고, 성립한다면 상기 콘텐트 M을 이용하는, 콘텐트 분배 방법.

청구항 9.

제 8 항에 있어서,

콘텐트 M이 불법적인 것으로 결정된다면, 콘텐트 M의 공급원은 상기 위탁 등록 기관에 의해 식별될 수 있는, 콘텐트 분배 방법.

청구항 10.

콘텐트 제공자(104)로부터 콘텐트 소비자(108)로의 콘텐트의 분배를 위한 장치로서,

콘텐트 제공자와 연관되며,

(i) 위탁 등록 기관(106)으로의 상기 콘텐트의 등록을 요청하고,

(ii) 상기 위탁 등록 기관으로부터 등록 정보를 수신하고,

(iii) 상기 콘텐트와 연결하여 상기 콘텐트 소비자에게 상기 등록 정보의 적어도 일부분을 분배하도록, 동작하는 장치를 포함하는, 콘텐트 분배 장치.

청구항 11.

콘텐트 제공자(104)로부터 콘텐트 소비자(108)로의 콘텐트의 분배에 이용하기 위한 하나 이상의 소프트웨어 프로그램들을 포함하는 기계-판독가능 매체를 포함하는 제조 물품으로서,

상기 소프트웨어 프로그램들은, 실행되었을 때,

위탁 등록 기관(106)으로의 상기 콘텐트의 등록을 요청하는 단계,

상기 위탁 등록 기관으로부터 등록 정보를 수신하는 단계, 및

상기 콘텐트와 연결하여 상기 콘텐트 소비자에게 상기 등록 정보의 적어도 일부분을 분배하는 단계를 수행하는, 제조 물품.

청구항 12.

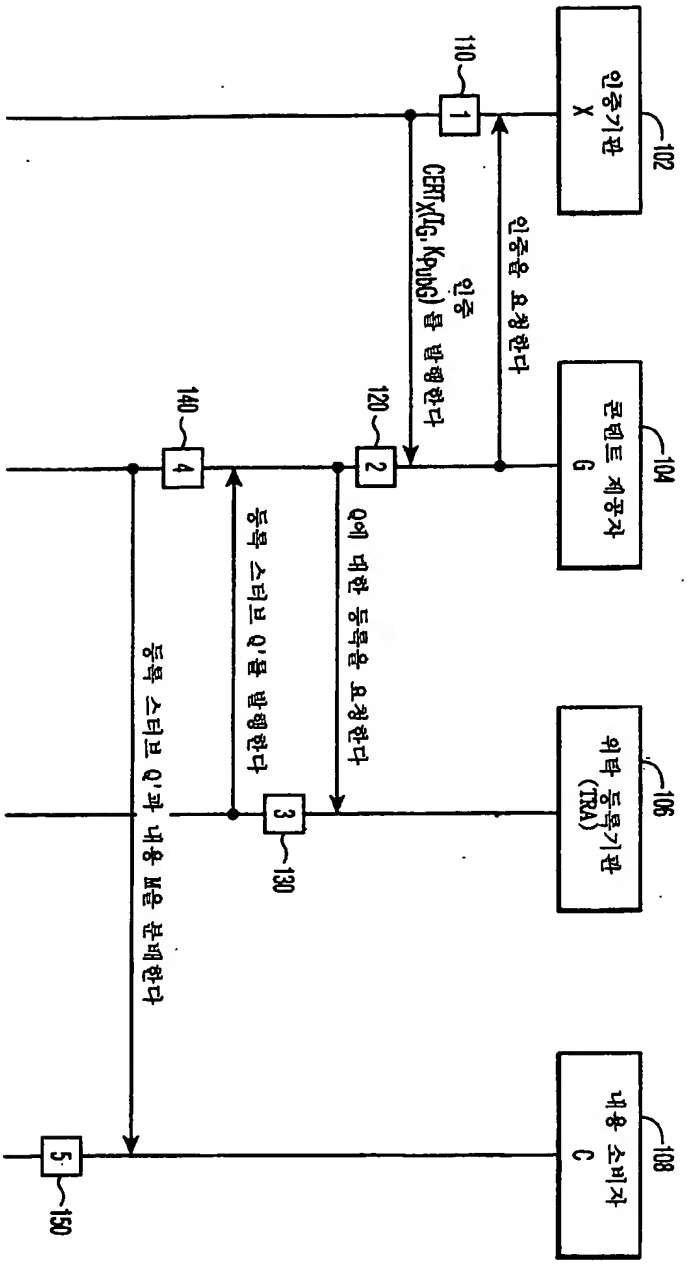
콘텐트 제공자(104)로부터 콘텐트 소비자(108)로의 콘텐트의 분배에서의 이용을 위해 등록 정보를 발생시키기 위한 방법으로서,

위탁 등록 기관(106)으로의 상기 콘텐트의 등록을 위한 요청을 수신하는 단계와,

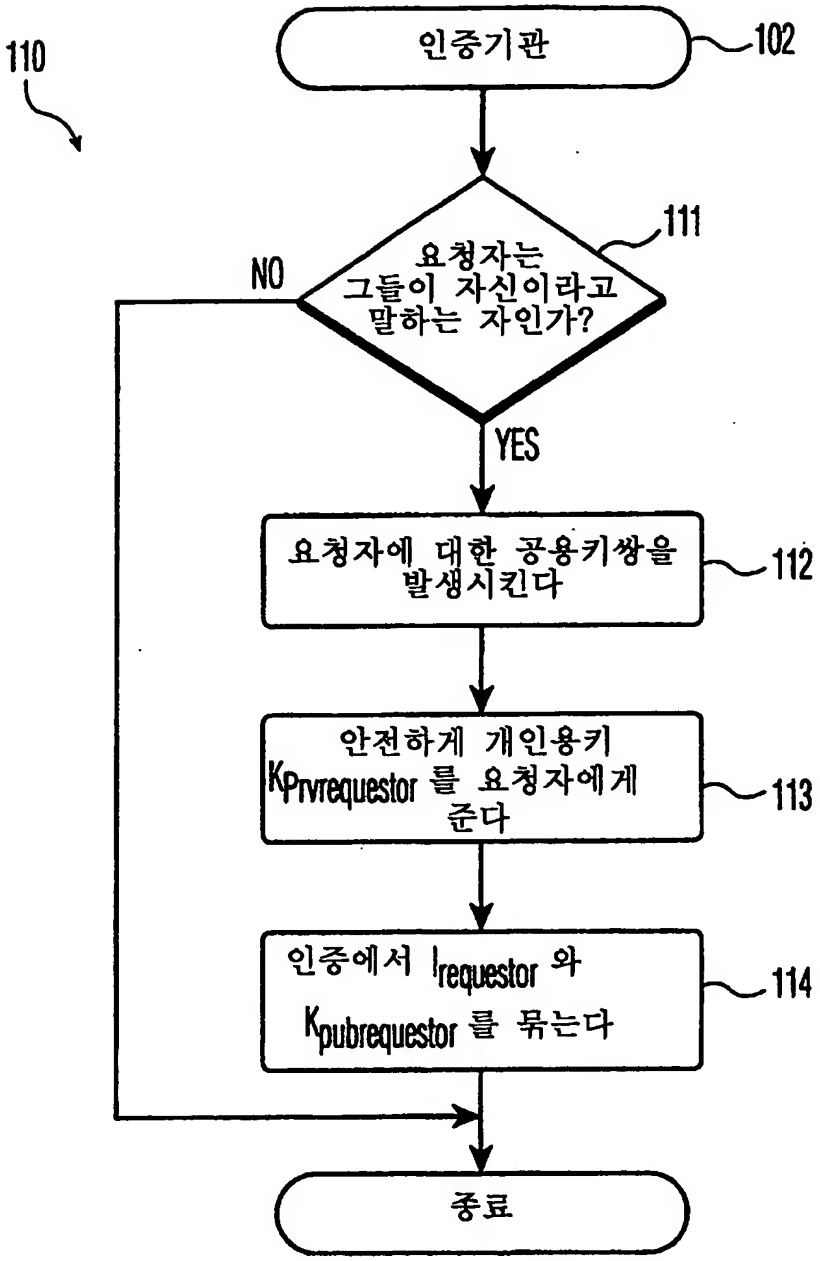
상기 위탁 등록 기관에 의해 발생된 등록 정보를 상기 콘텐트 제공자에게 전송하여, 상기 콘텐트 제공자는 상기 콘텐트와 연결하여 상기 콘텐트 소비자에게 상기 등록 정보의 적어도 일부분을 분배할 수 있는, 상기 전송단계를 포함하는, 등록 정보 발생 방법.

도면

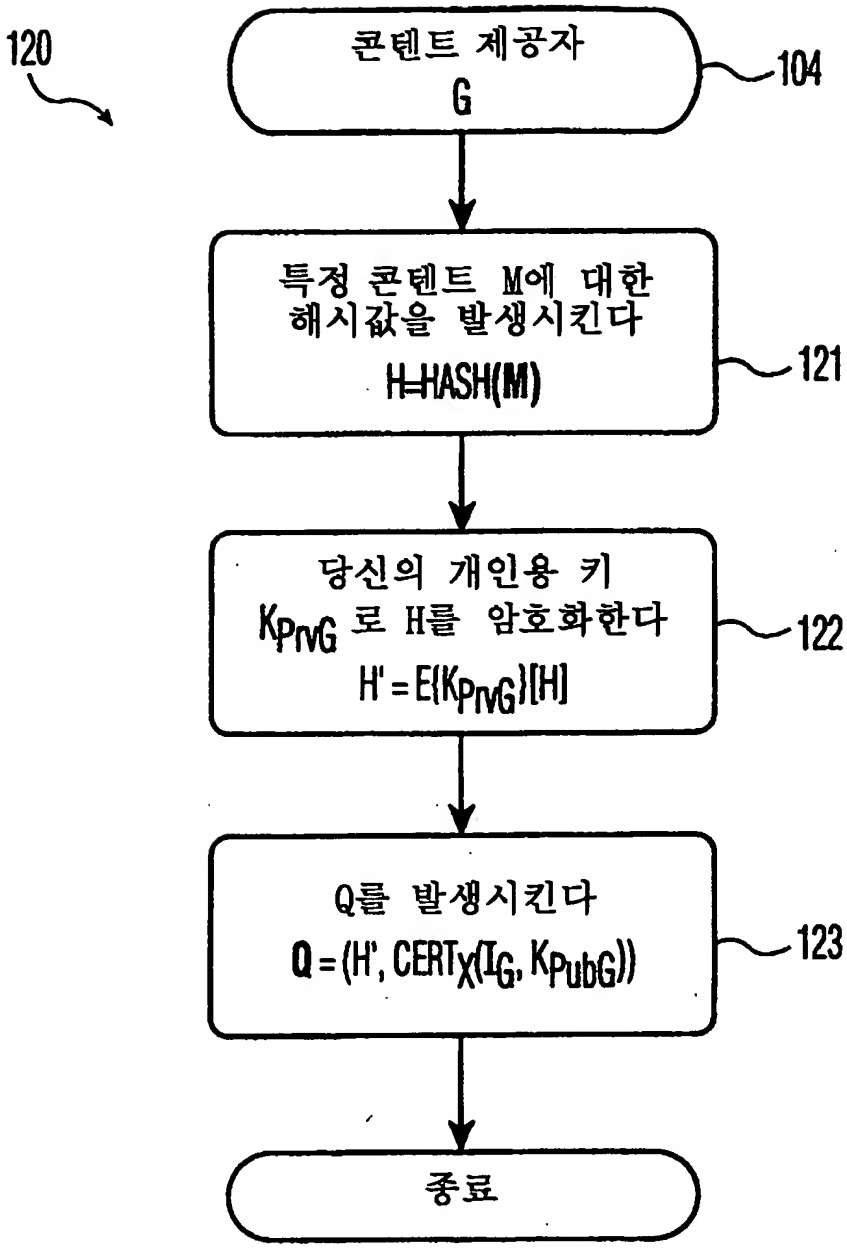
도면 1


인증기관
X
102
110
1
인증
CERT(X,G,K(PUBG))를 발행한다
인증을 요청한다
콘텐트 제공자
G
104
120
2
140
4
Q에 대한 등록을 요청한다
등록 스터브 Q'를 발행한다
위탁 등록기관
(TRA)
106
3
130
등록 스터브 Q'과 내용 M을 공개한다
내용 소비자
C
108
5
150

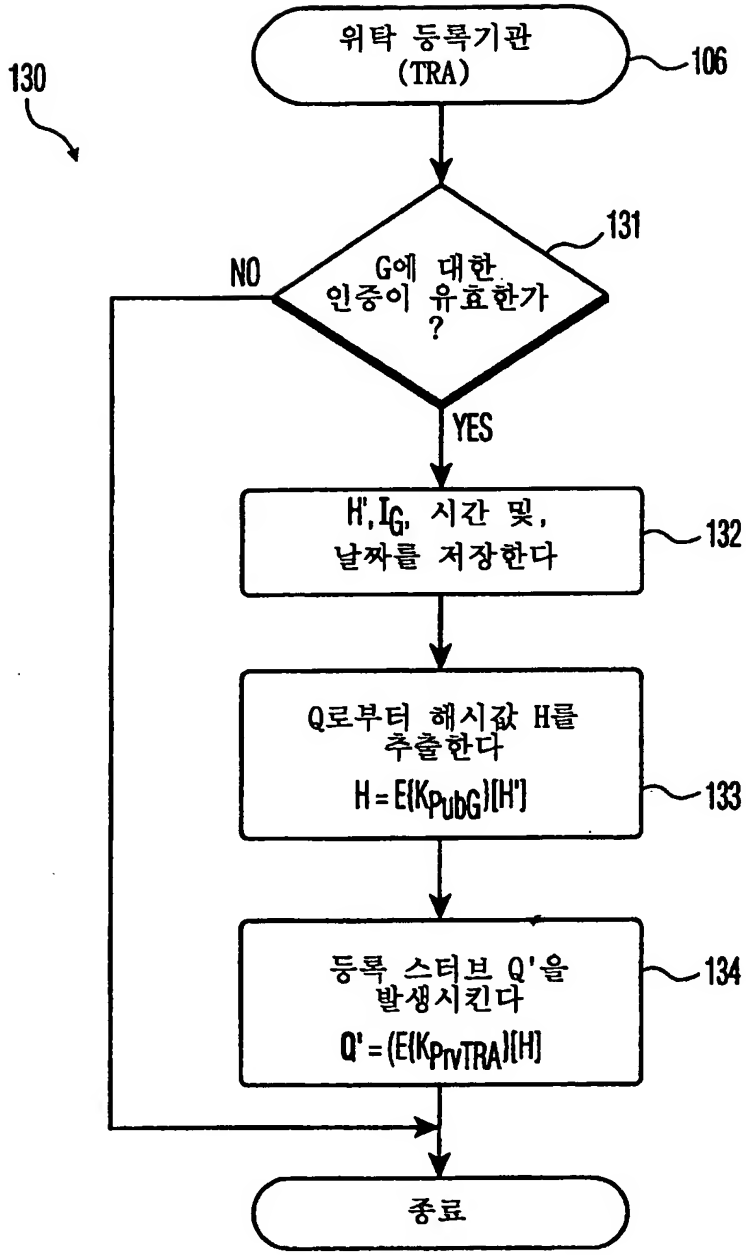
도면 2


110
인증기관
102
요청자는 그들이 자신이라고 말하는 자인가?
111
NO
YES
요청자에 대한 공용키쌍을 발생시킨다
112
안전하게 개인용키 $K_{Prvrequestor}$ 를 요청자에게 준다
113
인증에서 $I_{requestor}$ 와 $K_{pubrequestor}$ 를 묶는다
114
종료

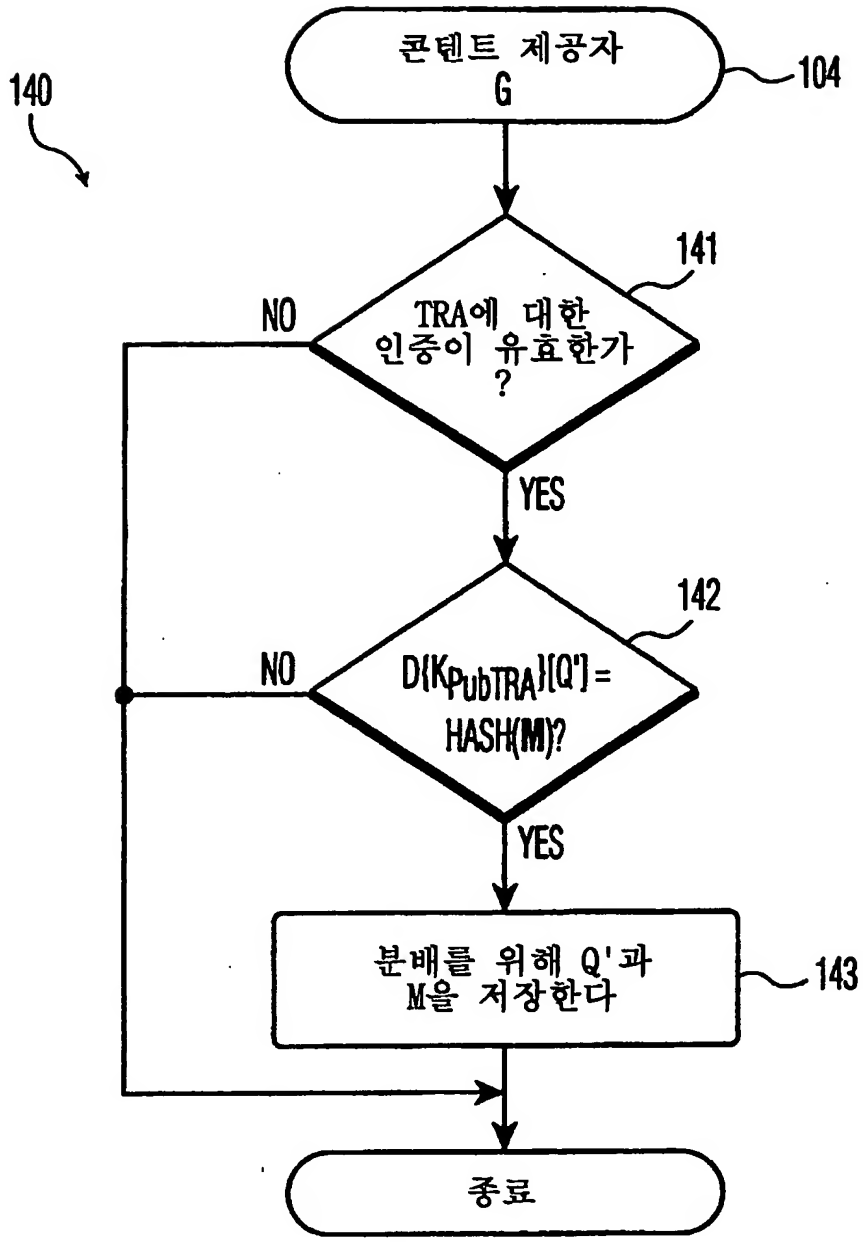
도면 3


120
콘텐트 제공자
G
104
특정 콘텐트 M에 대한
해시값을 발생시킨다
H=HASH(M)
121
당신의 개인용 키
K_{PrvG} 로 H를 암호화한다
$H' = E\{K_{PrvG}\}[H]$
122
Q를 발생시킨다
$Q = (H', CERT_X(I_G, K_{PubG}))$
123
종료

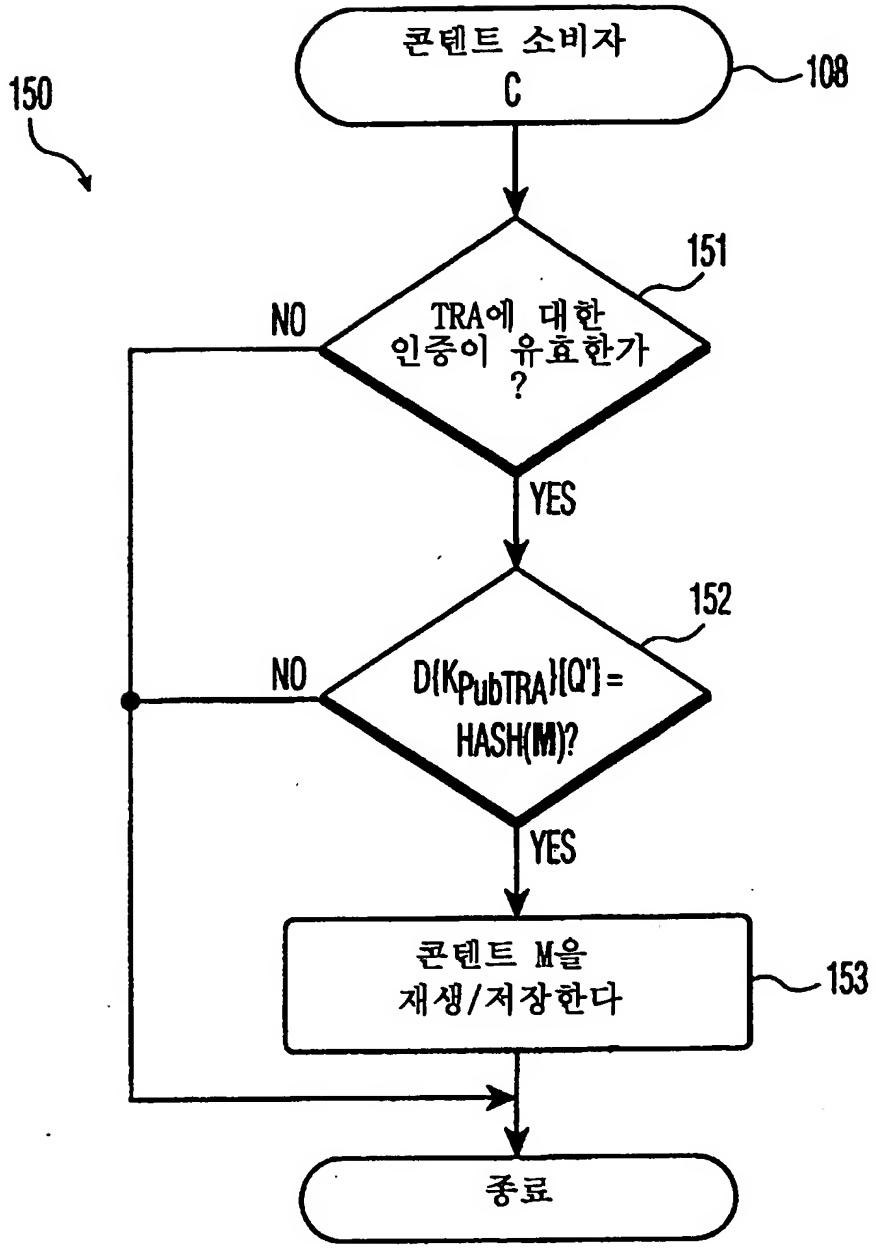
도면 4


130
위탁 등록기관
(TRA)
106
131
G에 대한
인증이 유효한가
?
NO
YES
H', I_G, 시간 및,
날짜를 저장한다
132
Q로부터 해시값 H를
추출한다
$H = E\{K_{PubG}\}[H']$
133
등록 스터브 Q'을
발생시킨다
$Q' = \{E\{K_{PrvTRA}\}[H]$
134
종료

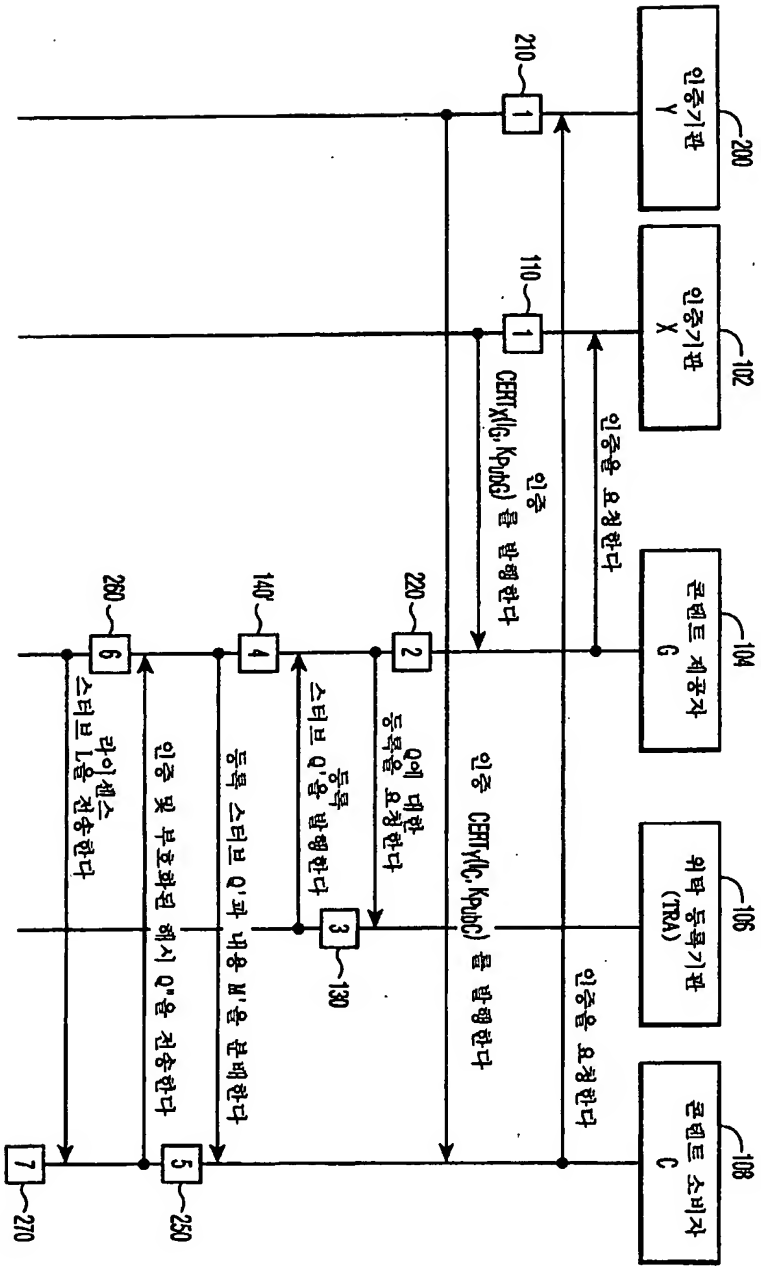
도면 5


콘텐트 제공자
G
104
140
141
TRA에 대한
인증이 유효한가
?
NO
YES
142
D[KPubTRA][Q'] =
HASH(M)?
NO
YES
분배를 위해 Q'과
M을 저장한다
143
종료

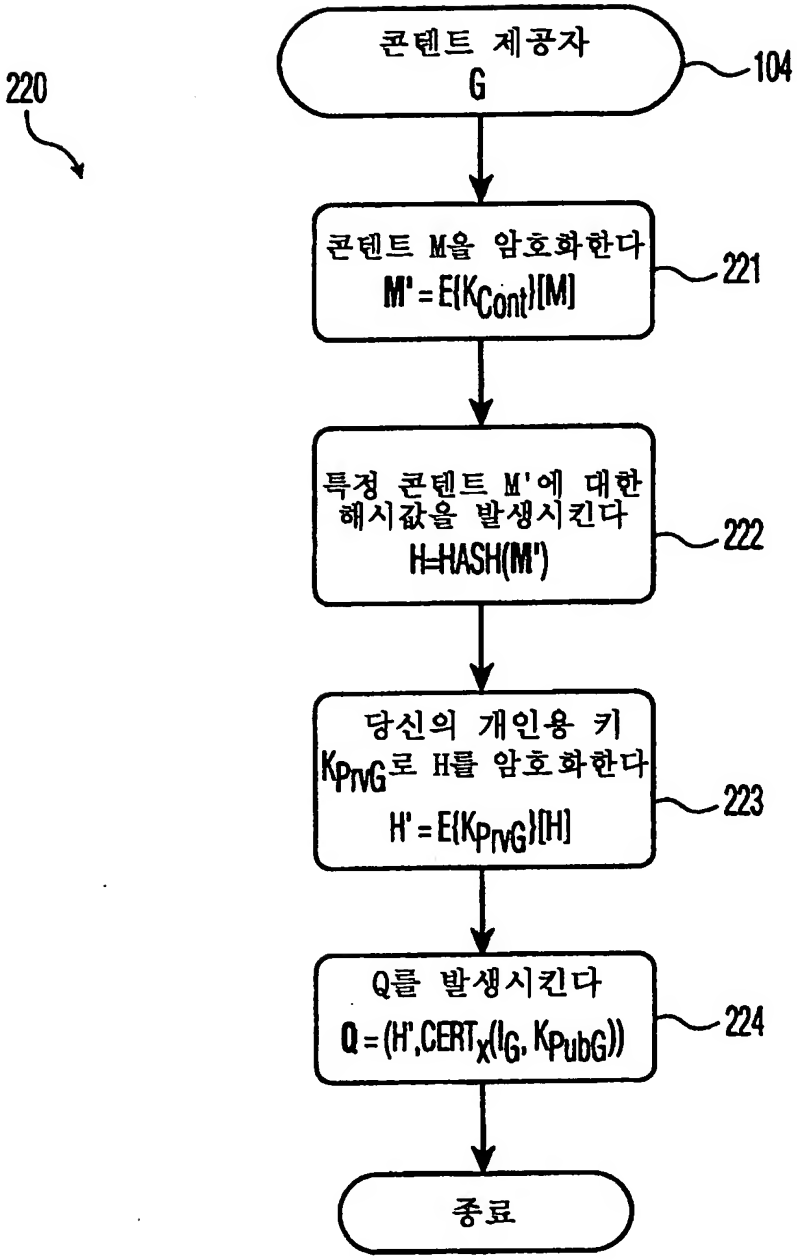
도면 6


150
콘텐트 소비자
C
108
151
TRA에 대한
인증이 유효한가
?
NO
YES
152
D{K_PubTRA}[Q'] =
HASH(M)?
NO
YES
콘텐트 M을
재생/저장한다
153
종료

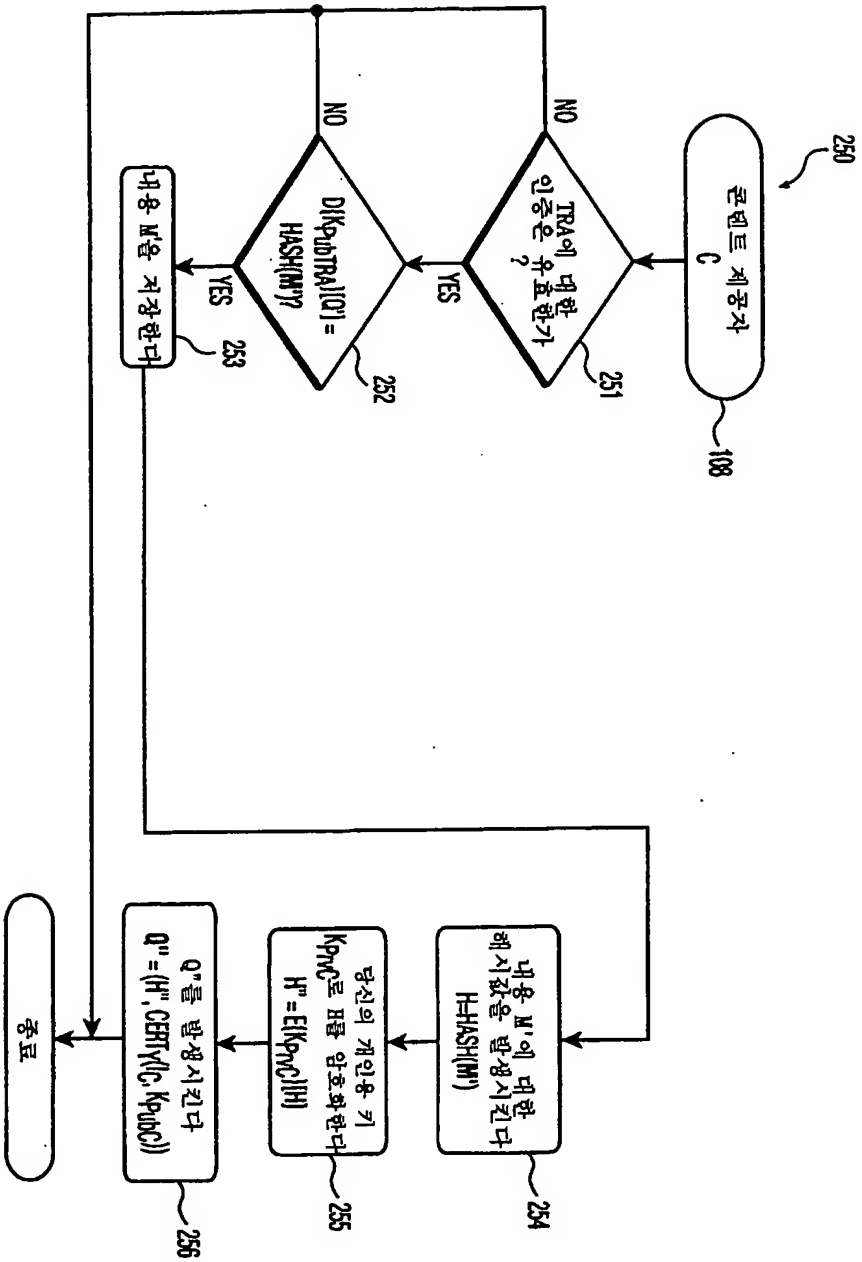
도면 7


인증기관 Y
200
인증기관 X
102
콘텐트 제공자 G
104
위탁 등록기관 (TRA)
106
콘텐트 소비자 C
108
210
110
220
140'
260
250
270
130
1
2
3
4
5
6
7
인증 CERTX(IC, KPUIC) 를 발행한다
인증 CERTY(IC, KPUIC) 를 발행한다
인증을 요청한다
인증을 요청한다
Q에 대한 등록을 요청한다
스티브 Q'을 등록 발행한다
등록 스티브 Q'과 내용 M'을 분배한다
인증 및 부호화된 해시 Q"을 전송한다
라이센스 스티브 L을 전송한다

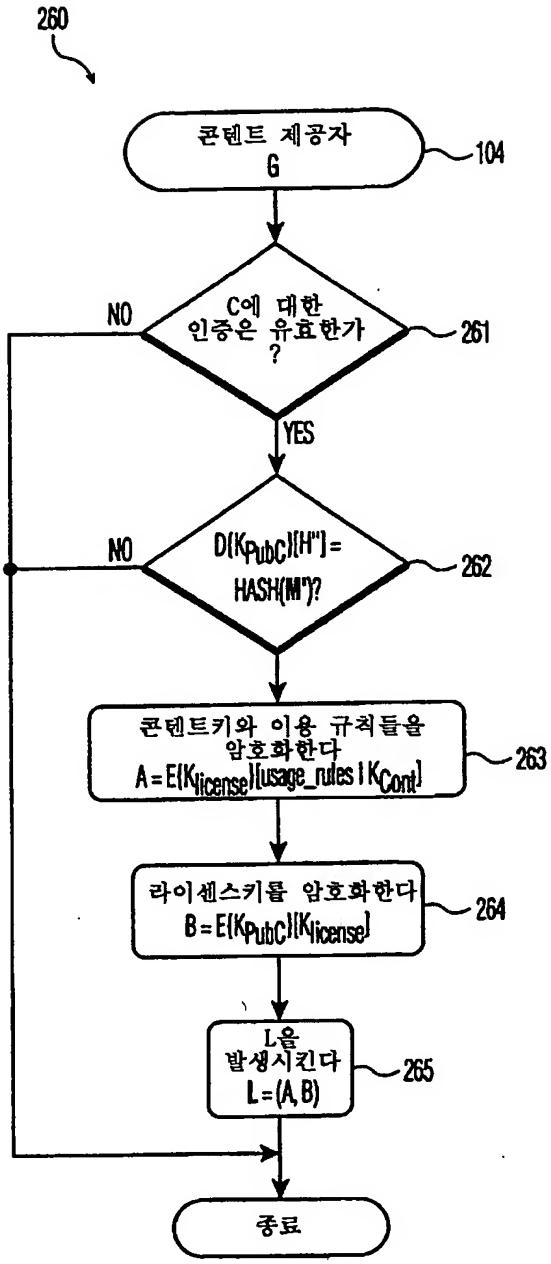
도면 8


220
콘텐트 제공자
G
104
콘텐트 M을 암호화한다
M' = E{K_Cont}[M]
221
특정 콘텐트 M'에 대한
해시값을 발생시킨다
H=HASH(M')
222
당신의 개인용 키
K_PrvG로 H를 암호화한다
H' = E{K_PrvG}[H]
223
Q를 발생시킨다
Q = (H', CERT_X(I_G, K_PubG))
224
종료

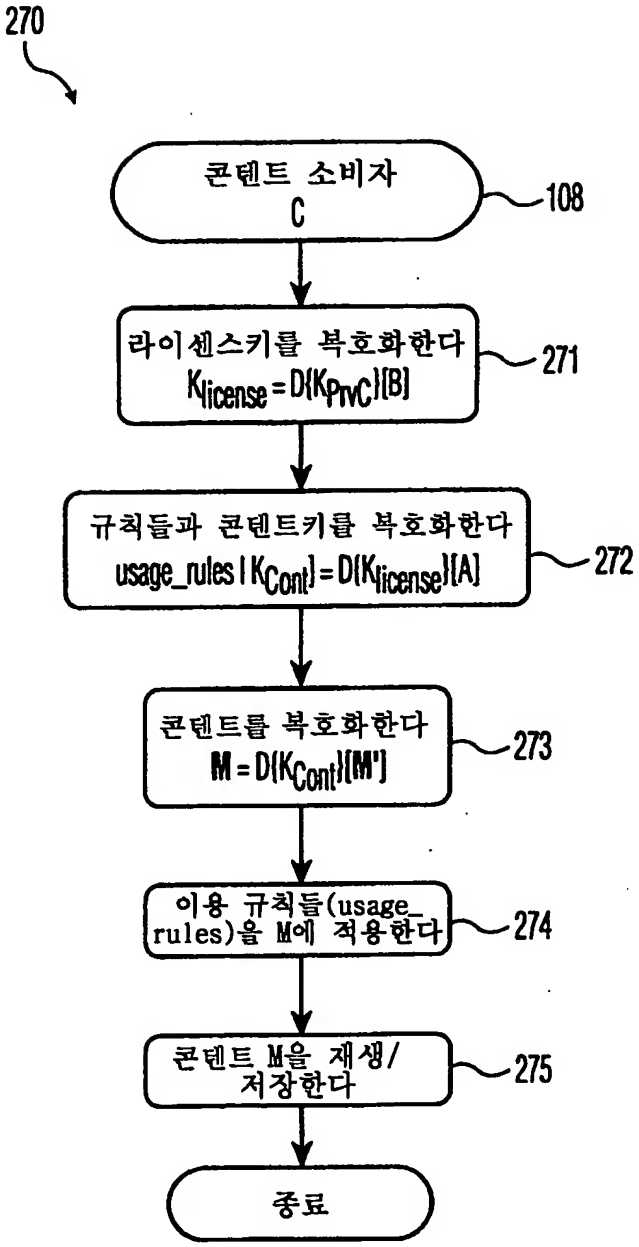
도면 9


콘텐트 제공자 C
250
108
TRA에 대한 인증은 유효한가 ?
251
NO
YES
DIK_PubTRA[[Q']] = HASH(M")?
252
NO
YES
내용 M'을 저장한다
253
내용 M'에 대한 해시값을 발생시킨다 H=HASH(M')
254
당신의 개인용 키 K_PrvC로 H를 암호화한다 H" = E[K_PrvC][H]
255
Q"를 발생시킨다 Q" = (H", CERT_V(C, K_PubC))
256
종료

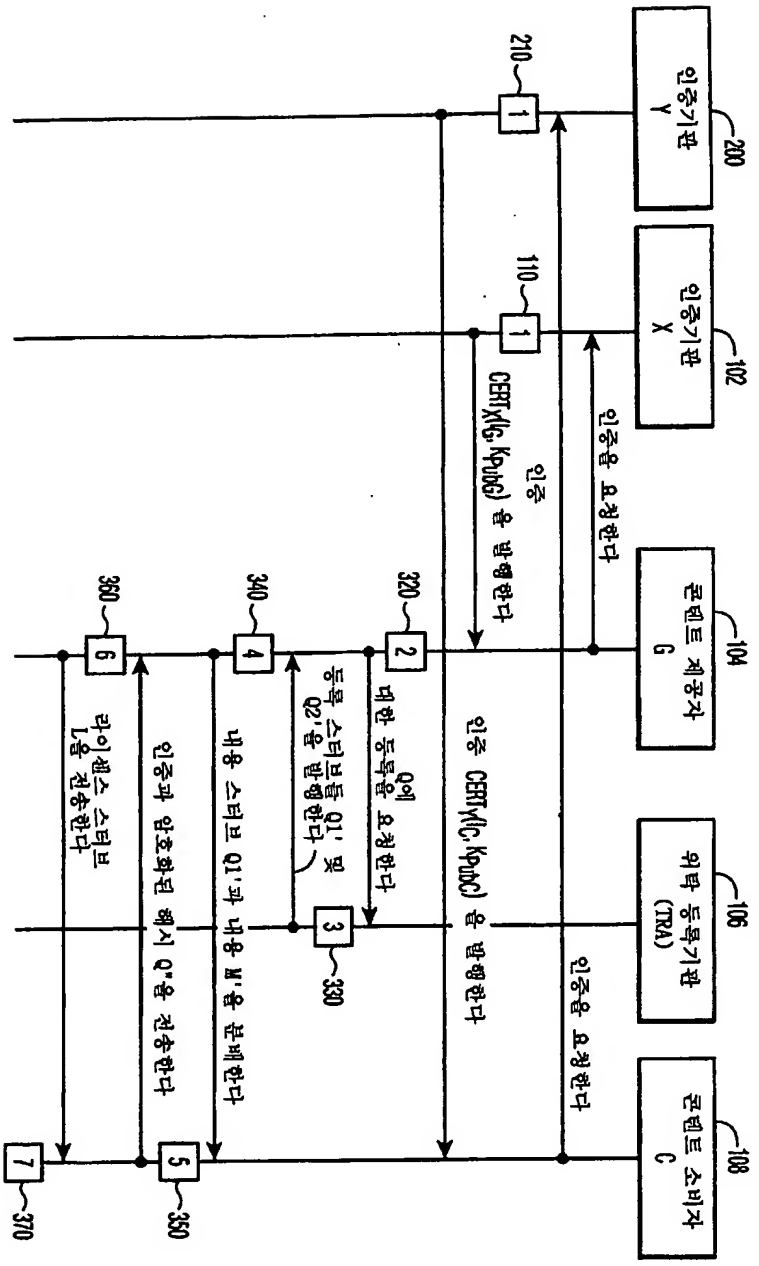
도면 10


260
콘텐트 제공자
G
104
C에 대한
인증은 유효한가
?
261
NO
YES
D(KPubC)[H"] =
HASH(M")?
262
NO
콘텐트키와 이용 규칙들을
암호화한다
A = E[Klicense][usage_rules | KCont]
263
라이센스키를 암호화한다
B = E[KPubC][Klicense]
264
L을
발생시킨다
L = (A, B)
265
종료

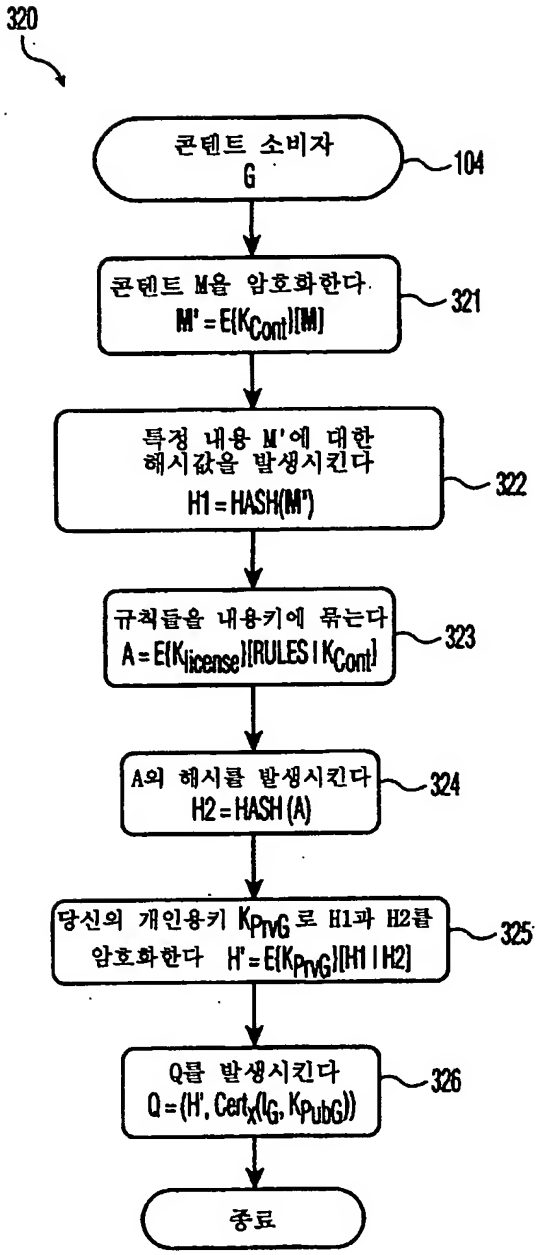
도면 11


270
콘텐트 소비자
C
108
라이센스키를 복호화한다
$K_{license} = D[K_{PrvC}][B]$
271
규칙들과 콘텐트키를 복호화한다
$usage\_rules \mid K_{Cont}] = D[K_{license}][A]$
272
콘텐트를 복호화한다
$M = D[K_{Cont}][M']$
273
이용 규칙들(usage_rules)을 M에 적용한다
274
콘텐트 M을 재생/저장한다
275
종료

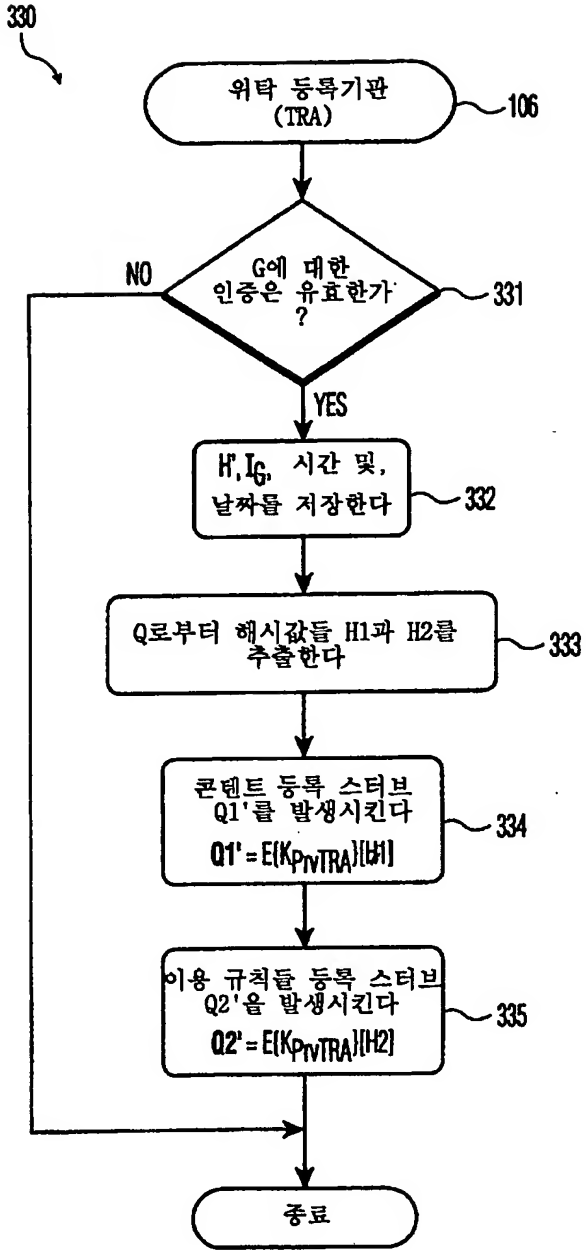
도면 12


인증기관 Y
200
210
1
인증기관 X
102
110
1
콘텐트 제공자 G
104
인증 CERT(G, KPUBG) 을 발행한다
인증을 요청한다
위탁 등록기관 (TRA)
106
콘텐트 소비자 C
108
인증 CERT(C, KPUBC) 을 발행한다
인증을 요청한다
320
2
C에 대한 등록을 요청한다
330
3
등록 스터브들 Q1' 및 Q2'을 발행한다
340
4
내용 스터브 Q1'과 내용 M'을 분배한다
350
5
인증과 암호화된 해시 Q"을 전송한다
360
6
라이센스 스터브 L을 전송한다
370
7

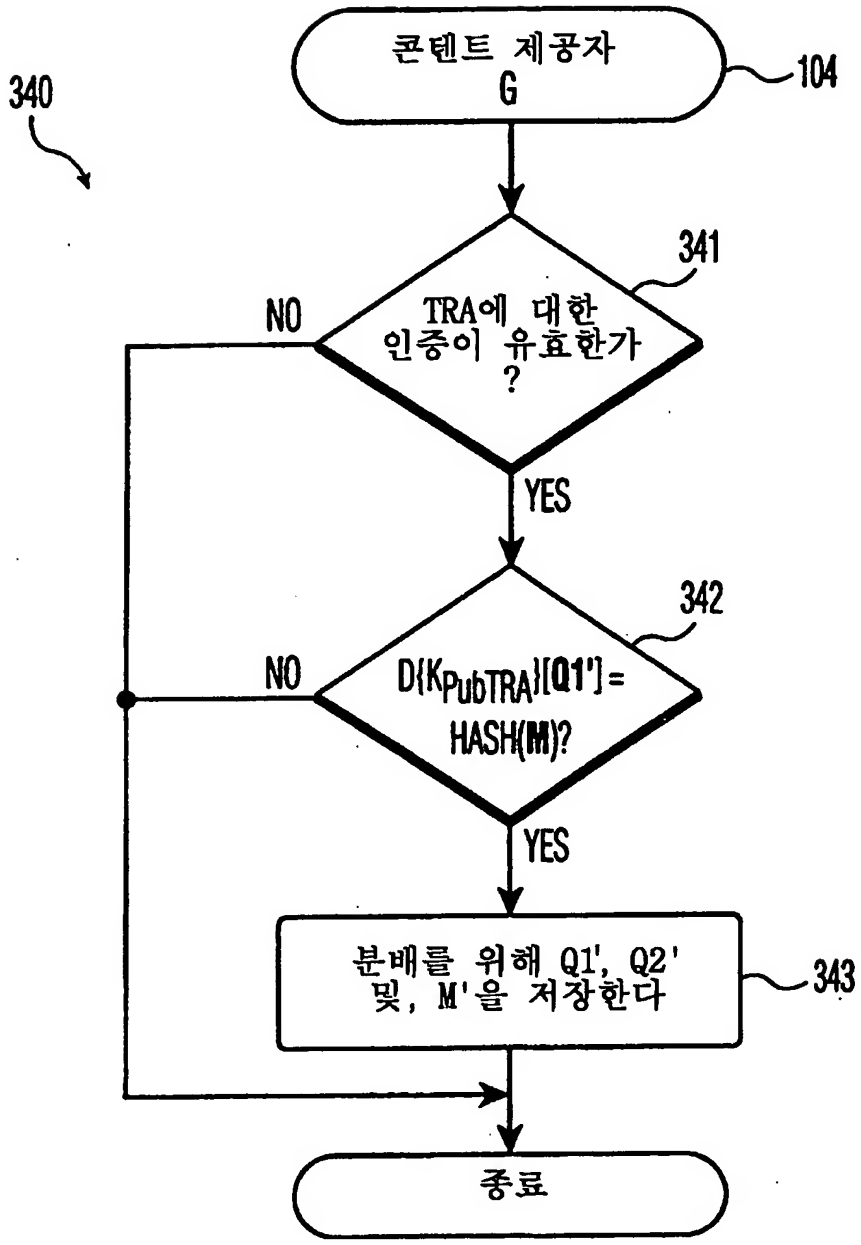
도면 13


320
콘텐트 소비자
G
104
콘텐트 M을 암호화한다
M' = E[K_Cont][M]
321
특정 내용 M'에 대한
해시값을 발생시킨다
H1 = HASH(M')
322
규칙들을 내용키에 묶는다
A = E[K_license][RULES | K_Cont]
323
A의 해시를 발생시킨다
H2 = HASH(A)
324
당신의 개인용키 K_PrvG 로 H1과 H2를
암호화한다 H' = E[K_PrvG][H1 | H2]
325
Q를 발생시킨다
Q = (H', Cert_X(I_G, K_PubG))
326
종료

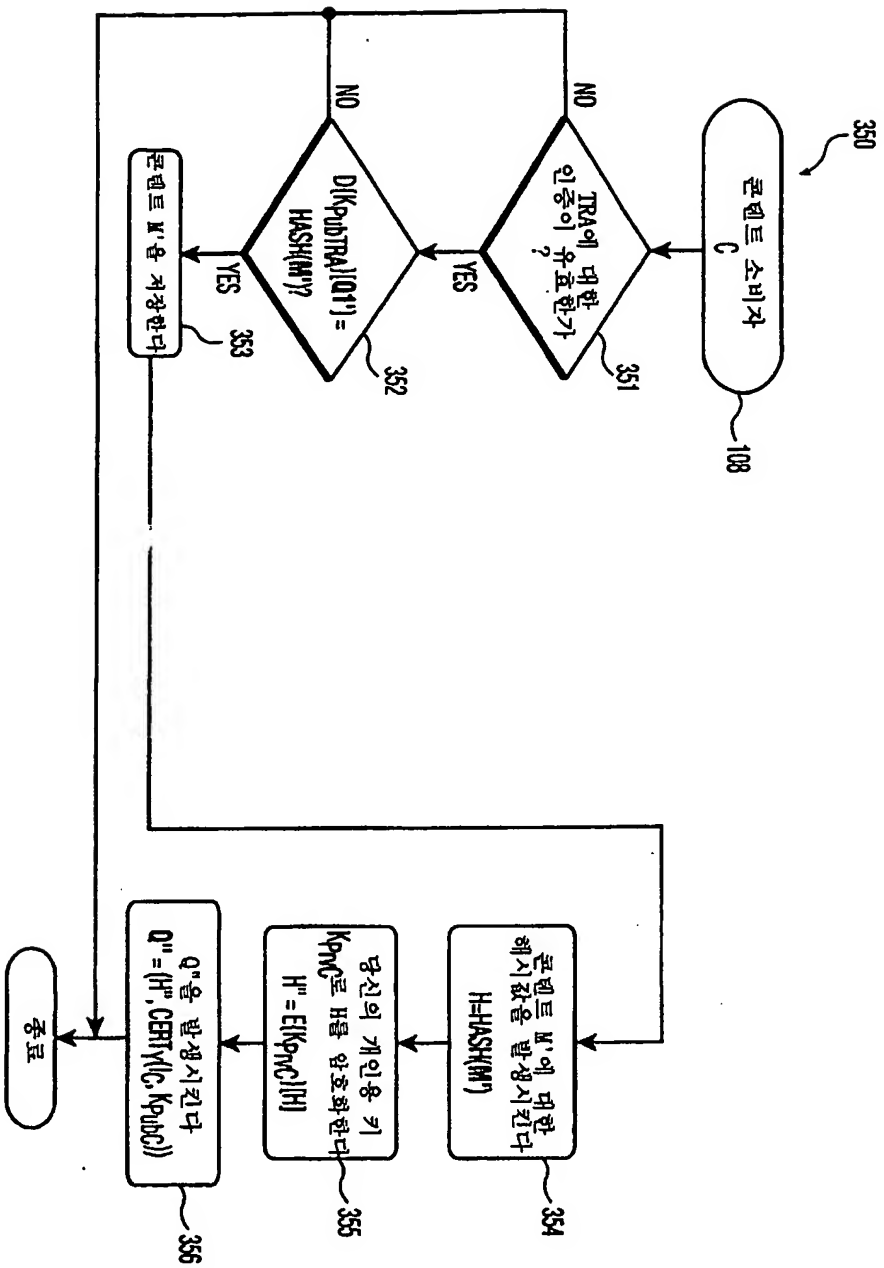
도면 14


330
위탁 등록기관 (TRA)
106
NO
G에 대한 인증은 유효한가 ?
331
YES
H', I_G, 시간 및, 날짜를 저장한다
332
Q로부터 해시값들 H1과 H2를 추출한다
333
콘텐트 등록 스터브 Q1'를 발생시킨다
$Q1' = E[K_{PTVTRA}][H1]$
334
이용 규칙들 등록 스터브 Q2'을 발생시킨다
$Q2' = E[K_{PTVTRA}][H2]$
335
종료

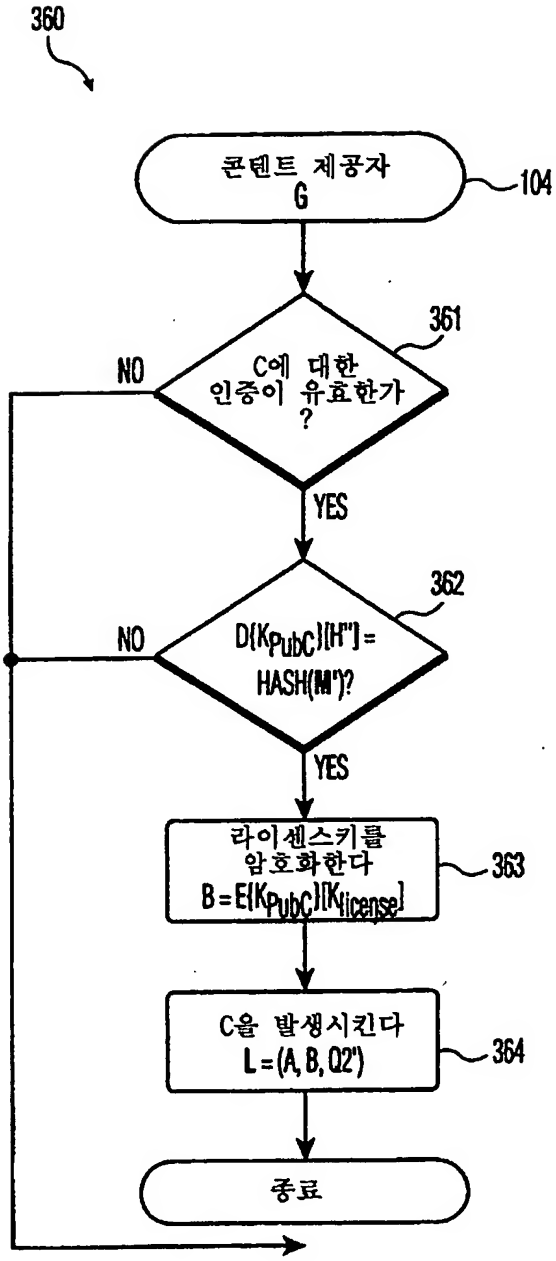
도면 15


340
콘텐트 제공자
G
104
341
TRA에 대한
인증이 유효한가
?
NO
YES
342
D{KPubTRA}[Q1']=
HASH(M)?
NO
YES
분배를 위해 Q1', Q2'
및, M'을 저장한다
343
종료

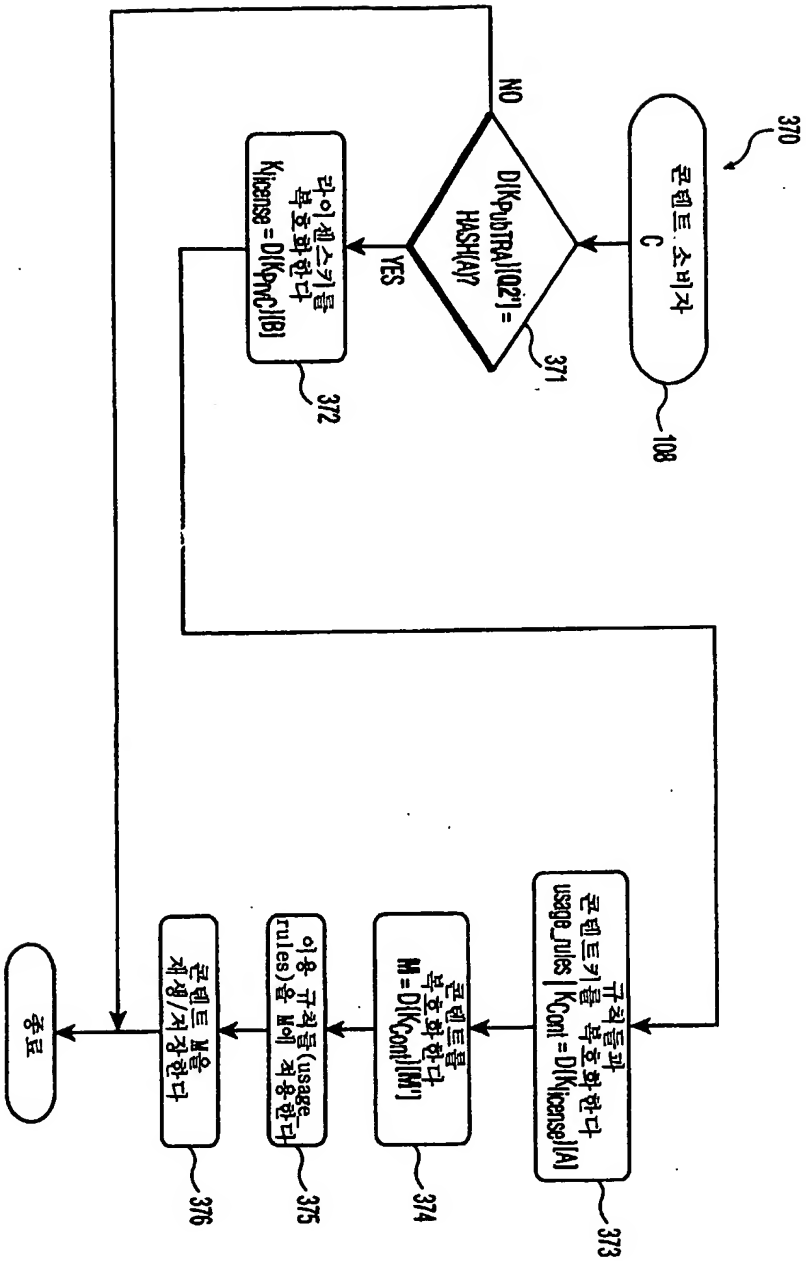
도면 16


콘텐트 소비자 C
108
350
TRA에 대한 인증이 유효한가 ?
351
NO
YES
DIKPUBTRA[IQ1'] = HASH(M')?
352
NO
YES
콘텐트 K'을 저장한다
353
콘텐트 M'에 대한 해시값을 발생시킨다
H=HASH(M')
354
당신의 개인용 키 KPRC로 H를 암호화한다
H" = EIKPRC[H]
355
Q"을 발생시킨다
Q" = (H", CERTIVIC, KPUBC))
356
종료

도면 17


360
콘텐트 제공자
G
104
361
C에 대한
인증이 유효한가
?
NO
YES
362
D[KPubC][H'] =
HASH(M')?
NO
YES
라이센스키를
암호화한다
B=E[KPubC][Klicense]
363
C을 발생시킨다
L=(A, B, Q2')
364
종료

도면 18


370
콘텐트 소비자 C
108
DIK_PUBTRA[102']= HASH(A)?
371
NO
YES
라이센스키를 복호화한다 K_license = DIK_PrvC[B]
372
규칙들과 콘텐트키를 복호화한다 usage_rules | K_Cont = DIK_license[A]
373
콘텐트를 복호화한다 M = DIK_Cont[M']
374
이용 규칙들(usage_rules)을 M에 적용한다
375
콘텐트 M을 재생/처리한다
376
종료